DDoS Capability and Readiness – Evidence from Australian Organisations

by

Ian Bernard Wiltshire

A thesis submitted for the fulfilment of the requirements for the degree of

Doctor of Philosophy

September 2022

Abstract

A common perception of cyber defence is that it should protect systems and data from malicious attacks, ideally keeping attackers outside of secure perimeters and preventing entry. Much of the effort in traditional cyber security defence is focused on removing gaps in security design and preventing those with legitimate permissions from becoming a gateway or resource for those seeking illegitimate access. By contrast, Distributed Denial of Service (DDoS) attacks do not use application backdoors or software vulnerabilities to create their impact. They instead utilise legitimate entry points and knowledge of system processes for illegitimate purposes. DDoS seeks to overwhelm system and infrastructure resources so that legitimate requests are prevented from reaching their intended destination.

For this thesis, a literature review was performed using sources from two perspectives. Reviews of both industry literature and academic literature were combined to build a balanced view of knowledge of this area. Industry and academic literature revealed that DDoS is outpacing internet growth, with vandalism, criminal and ideological motivations rising to prominence. From a defence perspective, the human factor remains a weak link in cyber security due to proneness for mistakes, oversights and the variance in approach and methods expressed by differing cultures. How cyber security is perceived, approached, and applied can have a critical effect on the overall outcome achieved, even when similar technologies are implemented. In addition, variance in the technical capabilities of those responsible for the implementation may create further gaps and vulnerabilities. While discussing technical challenges and theoretical concepts, existing literature failed to cover the experiences held by the victim organisations, or the thoughts and feelings of their personnel.

This thesis addresses these identified gaps through exploratory research, which used a mix of descriptive and qualitative analysis to develop results and conclusions. The websites of 60 Australian organisations were analysed to uncover the level and quality of cyber security information they were willing to share and the methods and processes they used to engage with their audience. In addition, semi-structured interviews were conducted with 30 employees from around half of those websites analysed. These were analysed using NVivo12 qualitative analysis software.

The difficulty experienced with attracting willing participants reflected the comfort that organisations showed with sharing cyber security information and experiences. However, themes found within the results show that, while DDoS is considered a valid threat, without encouragement to collaborate and standardise minimum security levels, firms may be missing out on valuable strategies to improve their cyber security postures. Further, this reluctance to share leads organisations to rely on their own internal skill and expertise, thus failing to realise the benefits of established frameworks and increased diversity in the workforce.

Along with the size of the participant pool, other limitations included the diversity of participants and the impact of COVID-19 which may have influenced participants' thoughts and reflections. These limitations however, present opportunity for future studies using greater participant numbers or a narrower target focus. Either option would be beneficial to the recommendations of this study which were made from a practical, social, theoretical and policy perspective.

On a practical and social level, organisational capabilities suffer due to the lack of information sharing and this extends to the community when similar restrictions prevent collaboration. Sharing of knowledge and experiences while protecting sensitive information is a worthy goal and this is something that can lead to improved defence. However, while improved understanding is one way to reduce the impact of cyber-attacks, the introduction of minimum cyber security standards for products, could reduce the ease at which devices can be used to facilitate attacks, but only if policy and effective governance ensures product compliance with legislation.

One positive side to COVID-19's push to remote working, was an increase in digital literacy. As more roles were temporarily removed from their traditional physical workplace, many employees needed to rapidly accelerate their digital competency to continue their employment. To assist this transition, organisations acted to implement technology solutions that eased the ability for these roles to be undertaken remotely and as a consequence, they opened up these roles to a greater pool of available candidates. Many of these roles are no longer limited to the geographical location of potential employees or traditional hours of availability. Many of these roles could be accessed from almost anywhere, at any time, which had a positive effect on organisational capability and digital sustainability.

Candidate Certification

I certify that the substance of this portfolio has not already been submitted for any degree and is not currently being submitted for any other degree or qualification.

I certify that any help received in preparing this thesis and all sources used, have been acknowledged in this portfolio.

Signature

Ian Bernard Wiltshire

Acknowledgements

I would like to thank my supervisors, Professor Sujana Adapa and Dr David Paul, for their unwavering support and guidance throughout my doctoral journey. Their encouragement, advise and praise, fuelled my confidence and guided me towards the completion of this thesis.

The University of New England, in particular the UNE Business school, Graduate Research School, and Research Services, were fundamental to the undertaking of this research project and I wholly appreciate the opportunity they provided to me. I would also like to thank Dr Philip Thomas and Professor John Rice for their support and openness as I found my feet as a HDR student.

To my wife Michelle and children, Audrey and Willow, thank you for your unconditional love and support over the past years. Your confidence in my abilities pushed me to persist in the face of long and arduous hours of research and writing. Your patience is admirable. I could not have done this without you.

I cannot thank my parents enough. I tried to complete in their lifetime. I only wish they could have stayed longer.

Thank you to all the willing participants who agreed to participate in my research. Your support and efforts came at a time of great difficulty and your participation is greatly appreciated.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
APEC	Asia-Pacific Economic Cooperation
B2B	Business to Business
B2C	Business to Customer
B2E	Business to Employees
B2G	Business to Government
BBS	Bulletin Board System
CIO	Chief Information Officer
CISO	Chief Information and Security Officer
COO	Chief Operating Officer
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name System
GDP	Gross Domestic Product
IoT	Internet of Things
ISO	International Standards Organisation
ISP	Internet Service Provider
LAN	Local Area Network
LoRaWAN	Long Range Wide Area Network
NTP	Network Time Protocol
SQL	Structured Query Language
WAN	Wide Area Network

DEFINITIONS

As this document discusses issues and threats at a technical cybersecurity level, I have included definitions of some of the terms used in this thesis so that all readers, regardless of technical capability or experience, can read and understand the contents and relevant contexts to which the information contained is applied. The definitions below are the common understanding of the terms.

Amplification DDoS Attack (sophisticated)

An attacker requests that a group of compromised IoT (Internet of Things) devices send a request for data (e.g., DNS requests or mail negotiation) to legitimate service providers. They spoof their send address as a target so that when legitimate responses are made, they are directed to the target instead of the actual source. A small (packet size) request becomes a larger reply to the target, hence amplification. The target is overwhelmed as resources become exhausted.

Antivirus

Software that monitors and inspects data either at rest or in transit in an attempt to match against patterns of known computer virus signatures.

Anycast

Anycast is an IPv6, one-to-nearest transmission method. With Anycast, multiple devices are configured to share an IPv6 address so that when an Anycast destination is requested, routing to that destination considers the shortest path to the closest instance of the request. For example, when requesting access to a website such as *YouTube*, the browser is directed to the instance that is closest to the device's current location via the shortest path.

Bit (b)

A single binary digit that can be either 1 (one) or 0 (zero). Network speeds are measured in Kbps, Mbps or Gbps, e.g., Telstra offers NBN at 80 Mbps download (80 Mb (megabits) = 10 MB (megabytes)) so a 10 Mb file will take 1 second to transfer.

Bits Per Second (bps)

A measurement of data transfer speed. A typical home internet connection of 30 Mbps can theoretically transfer a video of 4 GB in approximately 18 minutes. At 10 Gbps, the transfer would take a few seconds.

Bot/Botnet – (Robot) / Zombie

An internet-connected device that can be controlled remotely by unauthorised persons. They are collectively known as a network of bots (botnet).

Byte (B)

A group of 8 binary bits e.g., 10011010. Storage is measured in kB, MB, GB and PB

- kB – Kilobytes, where 1 kB is 1024 b (bits).
- MB – Megabytes, where 1 MB is 1024 kB.
- GB – Gigabytes, where 1 GB is 1024 MB.
- TB – Gigabytes, where 1 TB is 1024 GB.
- PB – Gigabytes, where 1 PB is 1024 TB.

Content Delivery Network (CDN)

A content delivery network is an online service that provides globally disbursed, load-balanced servers that are used to deliver content (video, audio, software) efficiently dependent on location of web server and remote requesting client.

Denial of Service (DoS)

The act of flooding a target system or device with bogus or unwarranted requests to prevent legitimate requests from gaining access to the destination.

Distributed Denial of Service (DDoS)

Distribution of many devices that participate en masse in a denial-of-service event.

Domain Name System (DNS)

DNS is supported by name servers that translate readable web addresses (e.g., www.une.edu.au) to routable Internet Protocol (IP) addresses (e.g., 202.9.95.188) and vice versa.

Internet of Things (IoT)

Devices that are connected to and may communicate through the public internet either openly or via virtual private networks (VPN).

IPv4

Internet protocol version 4 is a connectionless protocol that designates an address that enables communication between devices. Each unique (to network segment) address is composed of four binary octets (32 bits) that are commonly displayed in a readable dot decimal notation. It is usually accompanied by a subnet mask that determines which part of the address is the network and which part is the host. For example:
Dot decimal - IP = 58.104.180.56/20, Subnet Mask = 255.255.240.0.
Binary notation - 00111010.01101000.1011**0100**.**00111000** (hosts in green).
With a maximum of 32 bits available, IPv4 allows a maximum of just under 4.3 billion hosts. The example above is sub-netted to allow a maximum of 4,094 hosts per network.

IPv6

Internet protocol version 6 is a connectionless protocol that designates an address that enables communication between devices. Each unique (to network segment) address is composed of eight groups of four hexadecimal digits (16 bits) that are commonly displayed in a readable colon-separated hexadecimal notation. Due to the 32-character length, the address can be truncated by replacing groups of zeros with colons for easier readability. For example, 2001:c000:abcd:0000:0000:0000:0000:0000/48 can also be written as 2001:c000:abcd::/48. With 128 bits available, IPv6 allows a maximum of 2^{128} unique IP addresses.

Malware

Malware is software written to perform tasks or extract data without authorisation and can include trojans, spyware and encryption (ransomware).

Multicast

Multicast is a one-to-many transmission method. It allows one device to send to many devices without the network load that sending individually would create. For example, the provision of a webcast to 100 recipients would only require one video stream to be

sent from the hosting device. Multicast sends this video stream into the 100 destinations required (i.e., those who are members of the multicast group), with no additional load on the source device.

Packet

A unit/chunk of data that is encapsulated in routing and other information in order to be routed from source to destination. Under TCP (Transmission Control Protocol), packets can be error checked and the protocol ensures packets arrive in the correct order or orders a resend. Under UDP (User Datagram Protocol), packets are called datagrams. These do not have error checking capability so lost packets are not resent.

Packets Per Second (pps)

A group of bytes that form a unit of data. A typical standard is 1500 B (bytes), often noted as the maximum transmission unit (MTU) on network devices, although the maximum for TCP is 65,535 B (524,280 b).

Reflective Server

A server used to respond to requests for information such as web servers and DNS servers.

Volumetric DDoS Attack (low sophistication)

A low sophistication attack where the target is simply overwhelmed with many bogus, unwarranted and or erroneous requests that fill the bandwidth with the intent of denying a path for legitimate requests, e.g., flooding a server with ping requests.

Requests Per Second (rps)

A measure of the number of requests sent or received by a system or device. Requests are constructed using packets of data but as the data size differs depending on the request, there is no direct correlation between rps and pps. The amount of rps processed depends on the resources of the device and the complexity of the request.

Supply Chain Attack

Bad actors attempt to infiltrate vendors or smaller, less-protected connected organisations as a steppingstone to their larger intended target.

Transactions Per Second (tps)

A measure of a complete transaction usually applied to a more complex action or process request.

Virtual Private Network (VPN)

An end-to-end tunnel of encrypted network connection through the public internet. May use protocols such as TLS (Transport Layer Security), L2TP/IPsec (Layer 2 Tunnelling Protocol/Internet Protocol Security) or the older, less secure PPTP (Point-to-Point Tunnelling Protocol).

PHD JOURNEY

Attainment of a PhD degree requires the development of a thesis or dissertation in order that a candidate's research may be reviewed, assessed and defended before a degree is ultimately conferred. Countries such as the USA and the UK approach thesis and dissertation differently to the approach in Australia. In the USA, a thesis is submitted for a master's level degree and a dissertation is submitted for PhD degrees. Both of these documents are required to be defended before the degree is awarded. The UK follows the reverse, requiring a thesis be submitted for doctoral degrees and a dissertation to be submitted for a master's degree. Australia tends to settle on the thesis for PhD and permits a response to the review panel's comments without the need for oral defence. However, universities are reportedly interested in the possibility of introducing an oral defence process (Kiley et al., 2018).

The completion of this PhD has been challenging from several aspects. Completing a PhD requires considerable effort, focus and comfort with learning the many new methods and tools used in a research project of this size, but given the duration of the project, other events can arise to challenge even the most thoughtfully created plans. At the start of my PhD, I had planned to follow a path to complete a PhDI, which involves completion of a project portfolio within a workplace. Progress was initially good, with excellent results achieved. Unfortunately, approximately two years into my study, I suffered a family tragedy that was immediately followed by an employment status change, which meant the workplace project element became unattainable. As such and with much assistance from UNE, my supervisors and Higher Degree Research (HDR) Coordinator/s, my project pivoted and in 2019 I commenced this research-based PhD.

At the end of 2019, the COVID-19 pandemic occurred, which affected many people. My PhD studies were also impacted. While it was already very difficult to get staff from organisations to talk about cybersecurity for my data collection, COVID-19 removed the ability to perform interviews face to face, and finding willing respondents became even more difficult, perhaps due to the remote requirements of videoconferencing. Therefore, ethics approval needed to be revisited to obtain approval for alternate recruiting methods. As the country started to adapt to the

ongoing lockdowns and restrictions, progress began to pick up. Unfortunately, in early 2021, while still subject to closed borders, I suffered another family tragedy. Given that travel was still not permitted, I was grateful that we had the technology that allowed long distance communication.

Shortly after this, my home was flooded, which meant a further challenge to my resilience, as my work and research had to be conducted from a range of temporary accommodations. The difficulties I faced are not uncommon. Life is challenging and higher degree achievement is no exception. Completing a PhD is not a short task or a quick research project but rather a journey akin to an endurance race with the finish line some three to six years ahead. The duration of the project is such that the unexpected can and often happens and without immense commitment, unexpected challenges can threaten to derail even the most well thought-out and planned projects. However, the PhD is also a life journey and with support from family, supervisors and the university, while new knowledge is uncovered, personal growth can be amplified.

Chapter 1: Introduction

1.1 Introduction

Distributed denial of service (DDoS) can be a complicated form of cyber-attack to understand. To aid comprehension, imagine you are in a supermarket and there are 20 people in front of you, all with full shopping trolleys. They scan every single item, but when payment is required, they just walk out the door leaving the goods behind. This is DDoS – a distributed denial of service. Scaled up, there could be thousands of fake requests for service that are designed to tie up resources so that legitimate requests simply cannot get through. While this situation will likely be annoying for shoppers, imagine for a moment if the service being considered was not related to purchasing food but was the internet's Domain Name System (DNS) or another vital network service. Disruptions to these services can range from inconvenient to catastrophic. For example, customers may suffer the inconvenience of not being able to make ticket purchases if websites are offline but in the physical world, dam floodgates may fail to open when needed if instructions are prevented from reaching their target.

Despite the obvious direct disruption DDoS can cause, there can be other motivations. In the grocery analogy above, imagine that the store management team arrives to resolve the disruption and while they are focused on addressing the group occupying the check-outs, another group at the rear of the store are pilfering all the stock. This is another use for DDoS. When attacking a network, attackers may not always attempt to completely saturate a network connection. By ensuring that there is still enough bandwidth left for their activities, a DDoS attack can be used as a distraction to covertly steal Australia's personal, private and industry data along with valuable intellectual property.

Many of these consequences can be damaging to society and Australia's development strategy, which has global significance. Aware of its global impact, Australia has aligned its goals with the United Nations' (UN) Sustainable Development Goals (SDGs) (UN, 2018). There are 17 SDGs, many of which, such as food production, clean water, innovation in industry and infrastructure, and the sustainability of cities

and communities, can be impacted by interruptions to critical infrastructure (UN, 2022).

As DDoS is an easily accessible form of cyber-attack with a very low entry barrier, it stands as a credible threat to Australian industry. Therefore, it is necessary to gain a clearer understanding of the evolving DDoS phenomenon and the perceptions and understanding of employees in Australian medium and large-sized enterprises. This study aims to provide information that can help to understand the social implications of cyber-attacks and thus help to reduce the impact of these types of attacks on Australia's developmental progress.

This chapter begins with an overview of the research study, and discusses the background regarding DDoS and where the context of this research sits. Section 1.4 explains the research objectives and value and develops the three research questions, which were developed as the exploratory research proceeded. The significance of the original contribution is discussed in Section 1.5 and also included in the following section, Section 1.6, which provides an outline of the thesis. Finally, Section 1.7 presents a brief list of the publications and presentations delivered through the research process, and Section 1.8 provides a summary that concludes the first chapter and introduces Chapter 2.

1.2 Background

DDoS is a cybercrime that is currently on the increase (Kaspersky, 2021; Mansfield-Devine, 2015; Nazario, 2008), and while, historically, the reasons for most DDoS events were classed as vandalism (Bienkowski, 2016), statistics show that criminal activity such as extortion, activism and ideological disputes are now leading motivators (Berni, 2016; Constantin, 2021).

Supply chain attacks, where supporting industries are targeted to impact the intended victim, have increased and telecommunications carriers and data-related services are a focus for attacking groups (Netscout, 2021b). In the first three months of 2016, Akamai witnessed 4,523 DDoS attacks (Akamai, 2016), and it is of concern that this number seems to be growing (Akamai, 2016). In 2020, the number of DDoS attacks had risen to around 130,000 (Gutnikov, Badovskaya et al., 2021). In addition, the scale

of the attacks had also increased. The largest attack in 2016, which was against the DNS services organisation DYN, was 1.2 Tbps (Novinson, 2018), but in 2021, Microsoft experienced an attack that peaked at the much greater 3.47 Tbps (Kovacs, 2022).

In the initial documented observations of DDoS occurrences, costs incurred by the victim were limited to loss of productivity during the event (Radware, 2017; Smith, 2014). However, as incidents have increased in complexity and become more widely spread, these costs have escalated and assessment of damages resulting from an occurrence now considers a range of impacts:

- direct revenue loss (Kazerooni, 2015)
- reputational damage (Corero, 2016; Jackson, 2021)
- lost intellectual property or secrets (Jackson, 2021)
- ransom payments (Newman, 2021)
- legal costs (Jackson, 2021)
- cost to repair (Coenders, 2017)
- loss of productivity (Kazerooni, 2015)
- collateral damage to non-targets (Somani et al., 2016).

As DDoS relies on the availability of dispersed nodes, the relatively recent explosion of internet-connected devices, dubbed the 'Internet of Things' (IoT), has provided a rapidly expanding source of insecure endpoints (Millman, 2017) to compromise and marshal towards a target.

Furthermore, as it is apparent that direct (political or commercial) advantage may be extracted from delivery of DDoS attacks, groups have taken on commercialisation of the activity. This offering of 'DDoS as a service' delivers an ease of access to the general community with a simplicity that allows even school children to orchestrate an attack (Khalili, 2022). When combined with the relatively low cost of procurement, this may contribute to further increases in incidents. As such, the costs attributed to DDoS events are likely to increase as the scale, availability of comprisable nodes (Coenders, 2017; Rayome, 2017; Weagle, 2016) and commercialisation of delivery mechanisms increase (Orlowski, 2016; Smith, 2017).

1.3 Research Context

Initial research indicated that the extent of cybercrime is increasing in both scale and sophistication. Most organisations, if not all, experience daily threats in the form of:

- Phishing emails – deceptive emails sent with the aim of acquiring sensitive or personal information (Harrison et al., 2016) such as identity or financial data.
- Network port scanning – a process to search for active ports on a remote system so that known vulnerabilities can be exploited (Chauhan, 2018)
- Targeted attacks (intentional and accidental):
    - Targeted, such as data breach, ransomware and attacks aimed at disruption.
    - Accidental, such as poorly configured security that leads to exposure.

As stated by A10 Networks (2015), DDoS is an area of cybercrime that has been highlighted to be in a growth phase. This research project specifically targets DDoS as its subject of exploration.

An increase in cybercrime raises the risks for most businesses and organisations. However, the level of risk appears to be dependent on industry sector and location. For example, a recent report by Content Delivery Network (CDN) operator Akamai highlighted that the gaming industry was the major recipient of DDoS attacks throughout Q2 and Q3 of 2017 (McKeay, 2017, p. 10). Other reports concur with this statement, with only slight differences in the percentage distribution (Bender, 2014; CDNetworks, 2017). Publicly available targeted country information lacks consistency; however, as can be seen from the samples in Table 1.1, the United States of America and China consistently feature highly in the datasets from Incapsula and Kaspersky (Incapsula, 2016, 2017a, 2017b, Khalimonenko & Kupreev, 2017; Khalimonenko, Kupreev, & Ilgan, 2017).

Table 1.1

Sample of DDoS Targeted Country

Yr/ Qtr	Provider	1st	2nd	3rd	Australia position	Source
2019 Q2	Secure List	China 64%	USA 17%	Hong Kong 5%	9th	Kupreev, Badovskaya, and Gutnikov (2019b)
2019 Q1	Secure List	China 55%	USA 22%	Hong Kong 11%	10th	Kupreev, Badovskaya & Gutnikov (2019a)
2018 Q3	Secure List	China 77%	USA 12%	Australia 2%	3rd	Kupreev, Badovskaya, & Gutnikov (2018)
2018 Q1	Secure List	China 59%	USA 18%	South Korea 8%	>10	Khalimonenko, Kupreev, & Badovskaya (2018)
2017 Q3	Incapsula	Hong Kong 31%	USA 19%	Germany 13%	>10	Incapsula (2017a)
2017 Q3	Secure List	China 63%	USA 13%	South Korea 9%	>10	Khalimonenko, Kupreev, & Ilgan (2017)
2017 Q1	Incapsula	USA 92%	UK 2%	Japan 2%	8th	Incapsula (2017b)
2017 Q1	Secure List	China 48%	South Korea 26%	USA 9%	>10	Khalimonenko & Kupreev (2017)
2016 Q3	Incapsula	USA	UK	Japan	>10	Incapsula (2016)
2016 Q3	Secure List	China 72%	USA 13%	South Korea 6%	>10	Kupreev, Strohschneider, & Khali (2016)

Explanation of these observed differences may be due to the statistics being derived directly from monitoring equipment that is controlled by each report authoring organisation rather than a singular organisation that has statistics from all available countries. As such, if more data could be collected and analysed, a fuller, more complete picture could be compiled. However, from these statistics (see Table 1.1), and in all cases, the attack percentages of the top targeted countries easily eclipsed that of second place (Khalimonenko, Kupreev, & Ilgan, 2017; Incapsula, 2017a). This anomaly may be due to the targeted attack occurring for a short period of time when related to the sampling period. For example, the Estonian Government DDoS event of 2007 (McGuinness, 2017) may have placed Estonia in the top spot for that quarter in the statistics recorded by Estonia's monitoring organisation; however, given the inconsistency of the statistics, it is very challenging to determine a common trend. In effect, the statistics highlight the unpredictable and reactive nature of the phenomenon. This observation is supported by evidence that the Estonian DDoS attack was a reaction to political actions and inaccurate news reporting (McGuinness, 2017).

As Australia has been named in the top ten targeted countries (Table 1.1), it can be assumed that Australia is a valid target for DDoS, and therefore new research into the perception of DDoS of the Australian workforce is a valid and valuable proposition.

Incapsula (2017a) also highlighted ISPs (above gaming) as the leading attacked industry sector in Q3 2017. However, the order of the top ten list has not been consistent over time, and as Bjarnason (2019) and Imperva (2017) state, criminal motivations and the targeting of large transporters of wealth such as gaming and cryptocurrency appear to be increasing. It is therefore possible that any of the industry sectors listed in their reports could become a preferred target. Over recent years, reports of cyber events have highlighted a trend for conspicuous cyberattacks (such as DDoS) to be used as distractions while performing data theft (Ashford, 2016; Foltýn, 2019; Moses, 2013; Pauli, 2017). It can take many months to uncover the true target of what initially seems to be a disruptive event (Australian National University, 2019; Williams, 2019), and in some cases, the true target is never found or revealed (Williams, 2019).

While gaming and cryptocurrency hold value in direct finance, other organisations store wealth in the form of their intellectual property. Universities are a great example,

as they are in a sector that is publicly known for holding valuable research information (Westbrook & Blanchard, 2018), and these data are a key feature of their reputation. Similarly, there are many other companies that secure valuable intellectual property to safely protect them from competing organisations, political opponents and hostile countries (Remeikis, 2019; Reuters, 2015). Consequently, occurrences of espionage and corporate extortion have increased over recent years (Control Risks, 2017; Delibasic, 2018; Lindsey, 2019; McFarlane, 2017). As a prelude to a potential future opportunity, actual crimes have been surpassed by occurrences of criminals demonstrating their capabilities in order to secure future work or threaten those in competition (Ashford, 2016; Vishwakarma & Jain, 2019).

For criminals, businesses that hold valuable data could be considered valuable objectives; however, to make them a viable target, an available mechanism to deliver an attack must be in place. As seen with the Mirai botnet attack (Woolf, 2016), the mechanism relies on compromising distributed devices, such as insecure IoT units (Vishwakarma & Jain, 2019), to deliver the volumetric or sophisticated disruption that is appropriate to the chosen attack mechanism or strategy.

As ISPs have access to backbone networks that reach into distributed communities, these networks and the computer equipment they control have proved to be a valuable resource for the orchestrator of an organised objective (Constantin, 2015; Nichols, 2019). In a similar light, other businesses may also support a logical pathway to seemingly disconnected targets. Amazon Web Services (AWS), Google and Microsoft offer storage, computer and network services to a multitude of unrelated businesses, and a well-planned attack against these core services (such as AWS's Route 53 - Scalable DNS Service (AWS, 2019)) may result in enough widespread distraction (through publicly visible collateral damage) to camouflage any actual theft of targeted data.

The field of connected entities has been expanded (Priceonomics Data Studio, 2019) due to the fact that, in modern days, internet connectivity has become a utility rather than a luxury (Kang, 2016; O'Donnell, 2016). For internet service and cloud providers, greater accessibility underpins the growth of their sectors, and they seek to provide services that are attractive to all classes of business. The scalable nature of the service means that such services continue to be adopted by large and small businesses alike

(Kerner, 2019; Miller, 2019); however, the smaller firms do not have the staff and resources to focus on and actively monitor cyber-threats (Ward, 2015). Consequently, the lower protection provided within the smaller firms may serve as a less secure entry point to the larger firms that they have partnered with (Ward, 2015).

As larger firms tend to be able to generate additional profits through economies of scale (Kenton, 2019), they are able to use their pool of available resources to set up dedicated IT and cybersecurity departments. With the capacity to focus on cybersecurity, these IT and security departments can generate greater understanding and, thus, greater monitoring, alerting, mitigation and remediation plans for perceived threats. Therefore, it can be argued that larger organisations and core IT service providers should equally share the risk, knowledge gathering and understanding of potential DDoS threats. As shown in Figure 1.1, this research limits its field of focus to medium and large-sized Australian organisations (Australian Bureau of Statistics [ABS], 2010) that have designated IT departments and have staff that have some awareness of DDoS.

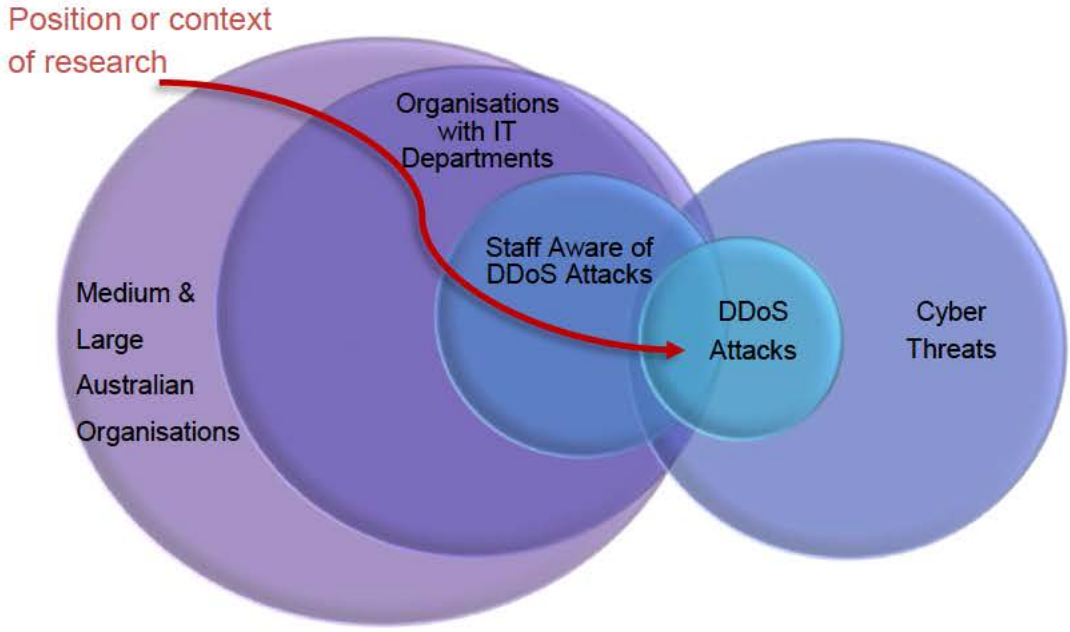


Figure 1.1. Contextual research positioning

1.4 Research Value, Objectives and Questions

This study provides valuable insights from practical, social and theoretical perspectives that lead to the formulation of appropriate research questions and research objectives for the study.

1.4.1 Research Value

Practical value

Practical value may be seen in the form of increased individual, organisational, industry and country preparedness for DDoS and other hostile cyber events. The knowledge uncovered may assist with the development of the plans, processes and training required to reduce the impact of an attack and to reduce the effort required during and post attack as teams deal with the consequential outcomes. Further, while this new knowledge may be easier for organisations with dedicated cybersecurity teams to act on and implement, those in smaller businesses without in-house capability or formal policy are equally able to extract value through their increased awareness of the topic.

Social value

As organisations increase the visibility of their corporate social responsibilities, the social value of a project becomes a key measure of its value to society. In 2022, the United Nations (UN) publicised its goals for sustainable development (SDGs) (UN, 2022). Of the 17 goals (which are discussed in greater depth in Section 6.6), nine could be impacted by the consequences of cyberattacks on Australian organisations, and while these goals have specific focus, they are all inextricably linked, as they each impact on areas other than their own.

- Zero hunger (SDG 2)
- Good health and well-being (SDG 3)
- Quality education (SDG 4)
- Clean water and sanitation (SDG 6)
- Affordable clean energy (SDG 7)
- Decent work and economic growth (SDG 8)
- Industry, innovation and infrastructure (SDG 9)
- Sustainable cities and communities (SDG 11)

- Partnership for the goals (SDG 17)

The UN's ninth SDG goal of sustainable industry, innovation and infrastructure focuses on areas such as transportation, industrialisation and infrastructure; however, this area also impacts on the production and distribution of food (zero hunger (SDG 2)), water treatment (clean water and sanitation (SDG 6)) and energy production (affordable clean energy (SDG 7)), all of which support good health and well-being (SDG 3). An attack that successfully disrupts one of these areas, such as the attack on the Maroochy sewage plant (Sayfayn & Madnick, 2017), could have a devastating effect on society both immediately and in the long term. The longer-term effects of significant disruption in these areas may also lead to impacts on sustainable cities (SDG 11) and the ability to find decent work (SDG 8), all of which fuel economic growth (SDG 8). At first glance, quality education (SDG 4) appears to stand alone; however, as innovation is heavily reliant on education (Diaconu, 2016), substantial disruption to the education sector has the potential to have a significant impact well into the future.

As a direct impact of the disruption caused by DDoS, medium and large-sized organisations that contribute to education, economic growth and sustainable cites may fail to deliver or suffer delays and quality reduction. Further, as demonstrated by the attack that shut down the US Colonial gas pipeline in April 2021 (Metcalf, 2020; Turton & Mehrotra, 2021), cyberattacks have demonstrated their ability to transcend their digital environment and impact on physical equipment, health, food, water and energy, which can experience extended and potential ongoing disruptions that have the potential to cause catastrophic outcomes for those affected.

Theoretical value

Although large quantities of research and information exist regarding the technical delivery, detection and potential mitigation of DDoS (Ghoshal, 2018; Groves, 2021; Hulme, 2019; Millman, 2017; Red Canary, 2021; Sucuri, 2019; Wueest, 2014), little has been written about individual and group perceptions and approaches to cyber-attacks such as DDoS. Theoretical value may be obtained from any hypotheses or theories generated from observations gathered throughout the study, and these may be used in the implications of the study and provide a base from which to perform future research.

1.4.2 Research Objectives

The primary objective of the study is to examine and understand the evolving perspective of the Australian IT workforce about the distributed cyber-threat known commonly as DDoS. While there are a number of existing commercial reports regarding DDoS that provide a global perspective (Table 1.2), most of these studies are concerned with methods of attack, methods of detection and methods of mitigation. For example, the reports by Kottler (2018) and Nicholson (2020) specifically discuss the timeline, methods, technology and motivation, and as with most studies, conclude with recommendations for monitoring and mitigation. There are few studies that offer knowledge about the motivation and if DDoS threat perceptions are in line with the realised risks.

Table 1.2

Sample of Commercial DDoS Reports

Reports
DDoS Attack Mitigation: A Threat Intelligence Report (Groves, 2021)
DDoS Attack Trends for 2020 (Warburton, 2021)
DDoS Attack Trends for Q4 2021 (Yoachimik & Ganti, 2022)
Global DDoS Threat Landscape Report (Imperva, 2021)
Quarterly DDoS and Application Attack Report (Radware, 2021)
NetScout Threat Intelligence Report (Netscout, 2021a)
State of the Internet: A Year in Review (Goedde, 2021)

While these reports do contain some valuable information for organisations that are seeking to further develop their defence strategies and high-level views, their scale and scope are limited, which reduces their ability to accurately depict the extent of the problem to any great depth and/or breadth. The reports contain analysts' generalised information, which this study finds to be a gap in current knowledge. By connecting directly with employees in organisations, knowledge from the inside can be uncovered to give a new, unique perspective.

1.4.3 Research Questions

The vast quantities of reading performed during the literature gathering and review phase highlighted areas where existing knowledge is scarce. As such, the research

questions were designed to find knowledge that is important and valuable to the research topic and that could be used as a platform that future research could be built on. The George Mason University and York University recommend that a research question must be clear, focused, concise, complex and arguable (George Mason University, 2018). However, research questions should also provide useful and worthwhile knowledge to those who will benefit from them (Mattick et al., 2018). Good research questions tend to be relatively narrowly focused and they help the research by providing a boundary that allows the research to be completed in a reasonable timeframe (Mattick et al., 2018).

The first research question for this study aims to understand if employees in medium and large Australian organisations consider DDoS to be a real and credible threat.

1. How high do Australian organisations rate DDoS as a threat when compared to other cybersecurity events?

To understand this question in more context, three subquestions were developed.

a) How is a DDoS threat evaluated?
b) What are the consequences of a DDoS?
c) Is a DDoS a large threat with low consequence or a low threat with large consequence or somewhere in between?

The second research question investigates the relationship between employee and employer.

2. Are Australian organisations and their employees aligned with regard to their perception of the threat of DDoS events?

Employees have their own intrinsic threat evaluation priorities but to understand how these impact on an organisation's security posture, understanding the dominant authority could help to understand more about the complexity of group motivations, hence the sub-question:

a) Is this perception led more by individuals or by organisational culture?

The final question seeks to uncover the concerns of employees, which are often hidden under the veil of the corporate public message. This question and sub-question seek a more raw and personal perspective of where to pursue improvements.

3. Where should effort be focused to ensure Australian organisations are more prepared for a DDoS event?

a) Where should effort be focused (by individuals, organisations, industry and government) to make the DDoS threat more widely understood by employees in Australian organisations?

1.5 Significance and Original Contribution

This study researches the perspectives of employees about cybersecurity and, specifically, the subcategory of DDoS. Initial exploration of the existing literature revealed that a large quantity of research and reference material is available concerning the technical aspect, with much of this focused on method, detection, avoidance and mitigation of attacks. Many technology-based articles have been produced by practitioner sources, such as Trend Micro, which discusses the technical cybersecurity risks of deploying IoT devices using LoRa (a long-range protocol) (Dudek, 2021). Academic sources included methods of detection (Jing & Wang, 2020; Li et al., 2018) and mitigation (Fenil & Kumar, 2019), such as the use of software-defined networking to create more effective mitigating defences (Swami et al., 2020). Additionally, some research has followed the path of attacker motivation with identification of motivators from an individual, organisational and state level. Mauslein (2014) and Thompson and Dreyer (2012) discuss how military size and a country's competitiveness affect levels of threat, and Hofstede et al. (2010) and Kolenko (2019) discuss how culture, social structures and community influence the security postures of individual groups. However, despite good coverage in these areas, little information is available on individual and group perceptions and approaches to cyber-attacks such as DDoS, especially from the perspectives of potentially targeted medium and large sized organisations employees. For these businesses, with the scale a reach of their organisations, DDoS remains a critical area of cyber-attack. These sized businesses (such as Universities, Hospitals and Government contractors) often hold large amounts of critical personal, private and sensitive information, which could be stolen when DDoS is used as a distraction method. In addition, millions of individuals could suffer from the direct impact of a DDoS attack and the resulting loss of services they rely on. This study aims to contribute to the body of knowledge, fill the identified void in the existing research and to help build a more complete understanding of this area of cybersecurity.

1.6 Thesis Outline

This thesis is organised into seven chapters and follows the traditional framework of introduction, methods, results, discussion and conclusion (IMRAD) (Heard, 2016), with this chapter forming Chapter 1 of that framework. Chapters 2 and 3 split the literature review into two parts.

Chapter 2 focuses on literature from industry to provide an external-to-organisation perspective on the way DDoS and other cyber-attacks have affected industry in the past and how they can potentially impact on society in the future.

Chapter 3 reviews literature from academic sources, which seeks to understand the phenomenon of DDoS in a cybersecurity context using objective reasoning and critical thought to present an understanding from country, organisation and individual perspectives. When consolidated, the practical and academic literature provide a solid review of the current knowledge of DDoS; however, the perspectives of both of these bodies of literature were constructed from an external 'looking in' perspective. This research study aims to identify perspectives from the alternate angle of inside (an organisation) 'looking out'.

Chapter 4 discusses the approach and methodology used to achieve that goal, including how the research was conducted during each phase and the methods and approaches to data analysis. This methods chapter is important as it allows future researchers to replicate any methods used to confirm the results and to allow them to transfer this methodical approach to new applications.

In Chapter 5, the results are provided with a brief description and discussion that will assist the reader to understand any relevant context. From a practical point of view, the discussion of the results in Chapter 6 highlights the new knowledge gained along with any considered implications of these new findings. This chapter eases the way for practical use of any theoretical recommendations and suggests directions for future research.

Finally, Chapter 7 concludes the thesis and offers some reflection on the study findings and research journey in a way that helps the reader gain a clear understanding of the key findings and arguments expressed through the main body of the thesis.

1.7 Research Presentations

During the course of this research journey, several publications and presentations were completed.

Three Minute Thesis (3MT) Competition

The aim of the University of New England's (UNE) 3MT presentation is for researchers to concisely describe their research project to a diverse audience in a three-minute timeframe (UNE, 2022a). Due to the restrictions in place during the COVID-19 pandemic, the 2020 competition was run remotely with entrants submitting an unedited video.

UNE Postgraduate Conference

The postgraduate conference aims to showcase higher degree research from across the university's academic disciplines (UNE, 2022b). For this conference, a 15-minute presentation was written to explain the basis of my research and current progress. At the conclusion, the abstract was published in the conference proceedings.

SEAANZ Annual Symposium

The Small Enterprise Association of Australia and New Zealand (SEAANZ) is a not-for-profit organisation that supports research into and dissemination of the understanding of small and medium-sized enterprises (SMEs) across Australia and New Zealand (SEAANZ, 2022). A paper and presentation that discussed how some of the findings from this research were relevant to SMEs were presented at the annual symposium in 2021.

ACSW Annual Conference

Australian Computer Science Week (ACSW) is an annual conference for researchers in computer science and other interested parties to gather and share their insights (ACSW, 2022). This conference presented an opportunity to disseminate the study's findings through the alternate medium of a poster submission.

For easy reference, these publications are presented in Table 1.3.

Table 1.3

Publication by Date

Date	Type	Title	Organisation
6 August 2020	Three Minute Thesis: Presentation	DDoS Capability and Readiness (https://www.youtube.com/watch?v=EB7Cbjmy9RI&ab_channel=GraduateResearchSchool%2CUNESABL)	UNE
23/24 June 2021	Postgraduate Conference: Abstract - paper presentation	DDoS Readiness and Capability (https://www.une.edu.au/__data/assets/pdf_file/0010/380359/2021-PG-Conference-Proceedings_Final.pdf)	UNE
11 November 2021	SEAANZ Symposium: Abstract - paper presentation	Pandemic Speed: Accelerating Innovation in Cyber Security	SEAANZ
November 2021	Book chapter acceptance	Wiltshire, I. B., Adapa, S. & Paul, D. (2022). Pandemic speed: Accelerating innovation in cyber security. In Adapa, S., McKeown, T., Lazaris, M. & Jurado, T. E. (Eds.) Small and Medium-Sized Enterprises, Business Uncertainty, Springer Nature, Singapore (Forthcoming).	
4 February 2022	ACSW: Abstract - poster	DDoS Readiness and Capability	ACSW

1.8 Summary

This introductory chapter set the context of the research, provided the background to the DDoS problem and explained how the study parameters were initially considered. Explaining the research value and original contribution, this chapter showed the practical relevance of the research and its significance in an academic setting. Section 1.6 discussed the approach to creating this thesis. Chapter 2 reviews the current literature assembled from practitioner sources.

Chapter 2: Literature Review – Practitioner

2.1 Introduction

This chapter reviews the literature sourced from industry-based authors and organisations. The chapter begins with a review of the growth of technology and how this growth aligns with the acceleration of the internet's adoption. A history of hacking and cyber-attacks is then added to show how these have grown in association with the adoption rates and technology advances. The innovation of the IoT is then introduced along with evidence to support its inclusion in cyber-attacks and the potential for use by criminal organisations. Following a historical journey through the significant DDoS events in history, the chapter covers details of common methods of DDoS attack before finishing with methods and approaches to detection and mitigation and practitioner viewpoints of information sharing and collaboration.

2.2 Technology

Technology continues to advance at an increased rate (Cassard & Hamel, 2018; Chandler, 2013). Kurzweil (2001) states that technology advances exponentially, and this appears to be a common view, with several laws of technology specifically supporting a prediction of exponential increases in technological capabilities. Moore's Law predicted that the number of transistors in an integrated circuit would double every two years (Moore, 1965), Kryder's Law considered the density of physical storage and predicted that storage density would improve much faster than processor capability (Walter, 2005) and Koomey's Law described a theory regarding computer power consumption, predicting that computing power needs would half every 18 months (Koomey, Berard, Sanchez, & Wong, 2011). However, while Moore's Law has appeared to follow the predicted growth pattern (as shown in Figure 2.1), there is evidence that Kryder's and Koomey's laws have failed to meet expectations.

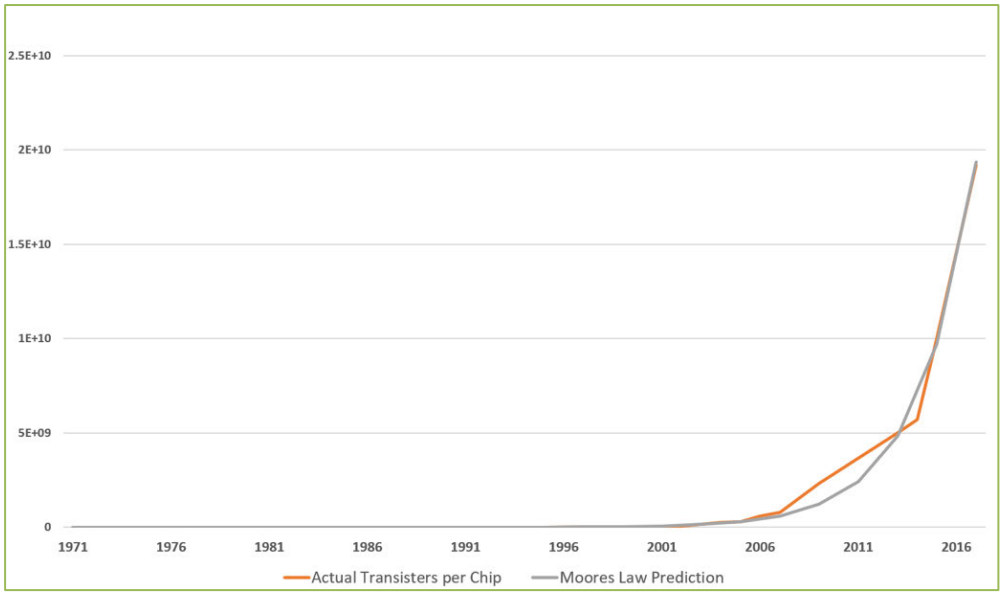


Figure 2.1. Moore's Law prediction vs actual (compiled from Rupp (2018))

Kryder's Law was a good predictor when the majority of storage disks consisted of magnetic media and storage was predicted to follow a path similar to Moore's Law, but the rate of increasing density fell short of predictions during the early 2000s. Since the move to solid state disks (SSDs) increased, Kryder's Law lost its relevance. Koomey's Law (Figure 2.2) also slowed but as environmental impacts pushed more focus onto reducing the power used by higher performing computers, Koomey's Law maintained its role in the prediction of power usage, even if the multiplier was reduced (Baxter, 2021). On closer inspection, Moore's Law also slowed, due in part to the costs involved with miniaturisation of transistors (Eeckhout, 2017). Therefore, this reduction in advancement with less transistor density than expected had the effect of influencing how closely Koomey's Law followed its own prediction for power consumption. Nevertheless, technology appears to be following an accelerated path of innovative growth.

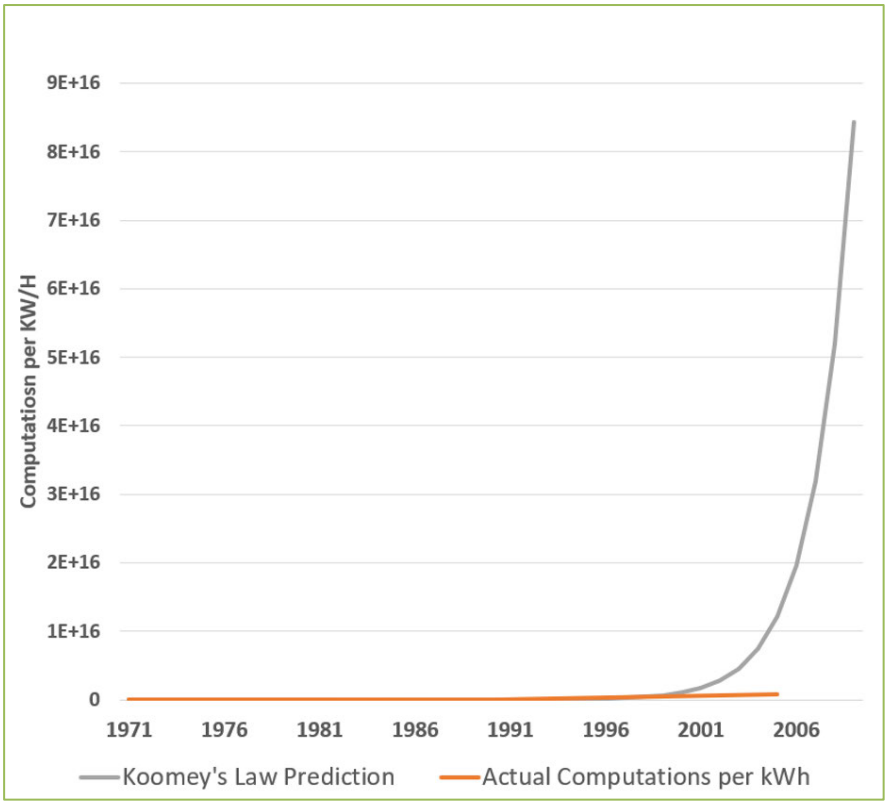


Figure 2.2. Koomeys Law prediction vs actual (compiled from Koomey et al. (2011))

New technology may not be solely reliant on faster and smaller integrated circuits. While efforts by integrated circuit manufactures are still advancing technology (Eeckhout, 2017), other innovators have found new ways to improve, such as pushing processing to data centres and away from the end user. Any slowing of Moore's and Koomey's laws, or even the lack of relevance of Kryder's Law with SSDs, appears to have not impacted on the rate of technology innovation, but it may influence how attackers who use DDoS plan their strategy. Therefore, in contrast with Kryder's Law, the development of DDoS cyber-attacks seems to have followed a similar growth curve to Moore's Law, is supported by Koomey's Law and has grown in a number of ways (Figure 2.3).

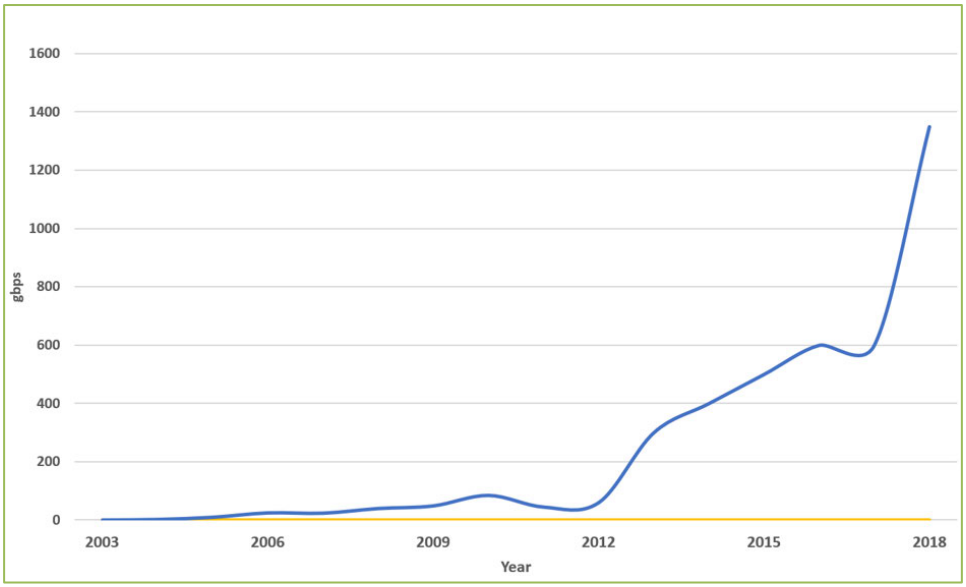


Figure 2.3. DDoS capacity growth over time (compiled from Cloudflare (2019), Jeftovic (2016) & Wang (2016))

Reports of DDoS attacks are now more numerous than a decade ago (Hulme, 2019; Jackson, 2019; Korolov, 2017; Rayome, 2019). Within these reports, DDoS capacity (Figure 2.3) (Cloudflare, 2019; Jackson, 2019; Jeftovic, 2016; Pitlik, 2019; Rayome, 2019; Wang, 2016), duration (Rayome, 2019) and level of sophistication (Pitlik, 2019; Rayome, 2019) are all reported to maintain steady growth as new ways are developed to deliver attacks (Hulme, 2019) and profit from the disruption caused (Cucu, 2019; Pitlik, 2019).

2.3 DDoS History

As the rate of DDoS technology change continues to accelerate (Hulme, 2019; Jackson, 2019; Korolov, 2017; Rayome, 2019), it is important to understand where the phenomenon originated, as analysing the trend of growth as well as the events and motivation behind attacks may make it possible to predict the future threat landscape (Quinn, 1967). Chronological examination of past events demonstrates how simple, mischievous fun for a teenager transformed into a global threat over a period of approximately 40 years (Dennis, 2010; Radware, 2017).

In the early days of shared computing, networks were confined to single rooms and buildings, with a central computer accessed through multiple terminal type devices.

This centralised topology allowed multiple end users to share an expensive central computational resource (Arzoomanian, 2009). The Computer Based Education Research Laboratory (CERL) at the University of Illinois was fortunate to participate in early computer innovation and developed the PLATO system (Programmed Logic for Automatic Teaching Operations), which was used to provide computer-assisted education support (Jones, 2015). At this laboratory in 1974, David Dennis, a 13-year-old with a passion for discovery, tested a command that was known to halt connected terminals. He expanded the known effect and wrote a software program to distribute the command, which affected 31 end users, forcing them to restart (Dennis, 2010; Radware, 2017). Therefore, an absence of malice but high levels of curiosity and exploration caused multiple users to be denied access, and the first denial of service (DoS) had occurred.

The modern form of DDoS relies solely on the existence of three components for an attack to be undertaken:

1. A source or person who is motivated to organise an attack.
2. A target that is connected and able to be reached.
3. A compromised network of devices (botnet) that has the capability to deliver the attack.

If any one of these three components is missing, the DDoS threat is nullified. A difference of opinion is all that is needed to provide the first two components and the existence of multiple interconnected devices and computers located around the world completes the picture. Without the modern internet, DDoS at the current scale would not exist, but the internet is a relatively new technological service that has been in existence for approximately 50 years, which means the levels of DDoS may still be in their infancy.

2.4 Rise of the Internet

In 1968, the USA's Advanced Research Projects Agency (ARPA) developed a packet switching network called Arpanet that connected government, tech companies and universities and transferred files via the ftp protocol (Norsar, 2016). In 1973, Norsar in Norway became the first connected site outside of the USA, and they sent seismic data to Virginia (USA) via satellite at a speed of 2.4 kbps (Norsar, 2016). Also in 1973,

a second satellite link from Kjeller (Norway) to London (England) was created, allowing transfer speeds of 9.6 kbps. In the early 1970s dial-up connectivity allowed single computer terminals to connect to a network using the Network Control Protocol (NCP) transport protocol (Figure 2.4., but it was not until 1983 that different networks could connect to each other. This technological advance was due to the development of the TCP/IP protocol (Transmission Control Protocol / Internet Protocol) (Norsar, 2016).

Figure 2.4. The internet in 1973 (from Newbury (2016))

At this point, due to the ability to 'internetwork' networks, Arpanet was widely considered to have transformed into what from then on was known as the internet (Figure 2.5).

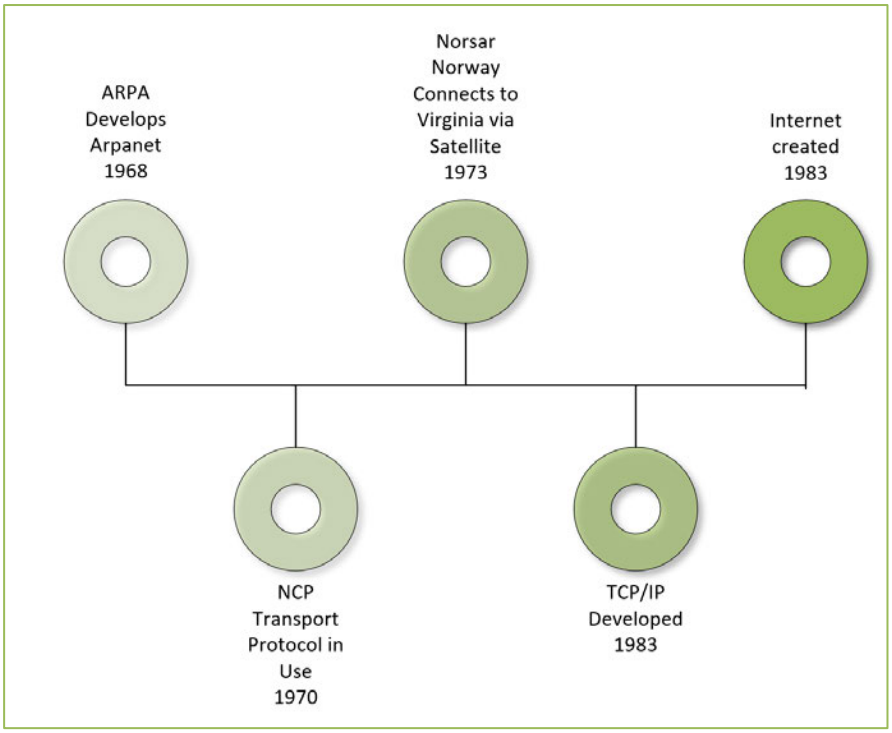


Figure 2.5. Internet timeline (by researcher)

2.5 Hacking for Fun

During the 1960s and 1970s, public groups of individuals explored and experimented with telecommunications equipment in an attempt to determine how telephone networks worked, which resulted in reverse engineering of the tone systems and the creation of electronic tone generators that could replay control commands and provide access to hidden areas of the network and, ultimately, free long-distance phone calls. At the time, this exploitation of the phone system was commonly called phreaking, and it was classed as a criminal act known as 'toll fraud' (Vocus, 2018). The rise in popularity of personal computers (PCs) and bulletin board systems (BBS), which were accessed via modem (a modulation/demodulation device) through the telephone network, provided a place where technology enthusiasts could meet and share experiences.

This rise in popularity coincided with technological advancements in telephone network electronic switching, and when the existing tone generators could no longer access the hidden tone channels, the BBS allowed 'phone phreaks' to discuss new methods of breaking into the networks (Kizza, 2017). Computer hackers who had an interest in computer networks rather than telephone networks also frequented the same

BBS, and as computers connected to networks via a modem, computer hackers copied the methods utilised by 'phreakers' to discover and record the telephone numbers of business modems for their future exploitation.

The movie *War Games*, which popularised the concept of computer hacking, was publicly released in 1983 (Brenner, 2010). It delivered stylised images of dial-up modems in use, which highlighted the apparent simplicity of accessing networks and from which network exploration could begin. In the movie, David Lightman (the main character in the film, played by Matthew Broderick) used auto-dial software to connect to every telephone number in his local area as he searched for access to play an as-yet unreleased computer game. He used this brute force attack method (also known as 'war dialling', which involves dialling every telephone number in a configured block) (McClure & Scambray, 1999) in an attempt to discover accessible networks and systems that had computers set to auto answer and would permit incoming connections. Once his connection was made, he could then explore the remote networks to see if any games could be accessed.

The movie portrays a child using technology to discover more games to play and could be considered exploration without malice. However, Lightman's innocent search for fun leads to a near global war, as through a series of events, the computer Lightman eventually accessed controlled the launch sequence for the USA's nuclear guided missiles. The impact of the movie and the potential for a catastrophic outcome motivated the USA to create their first internet policy (*Counterfeit Access Device and Computer Fraud Abuse Act 1984;* Schulte, 2008), and President Ronald Regan implemented the National Policy on Telecommunications and Automated Information Systems Security (The White House, 1984).

By the late 1990s, programming languages had advanced and were widely practised, with development of many of the languages that are still used today, such as Python, Ruby, JavaScript and PHP (Atwood, 2006). Internet adoption had grown to over 150 million users (Figure 2.6), which allowed innovators to become globally collaborative. Along with these innovators, computer hackers also found collaborative groups that united to pursue the lifestyle inspired by the various Hollywood dramatisations such as *War Games* (Cyber Security Masters Degree, 2018).

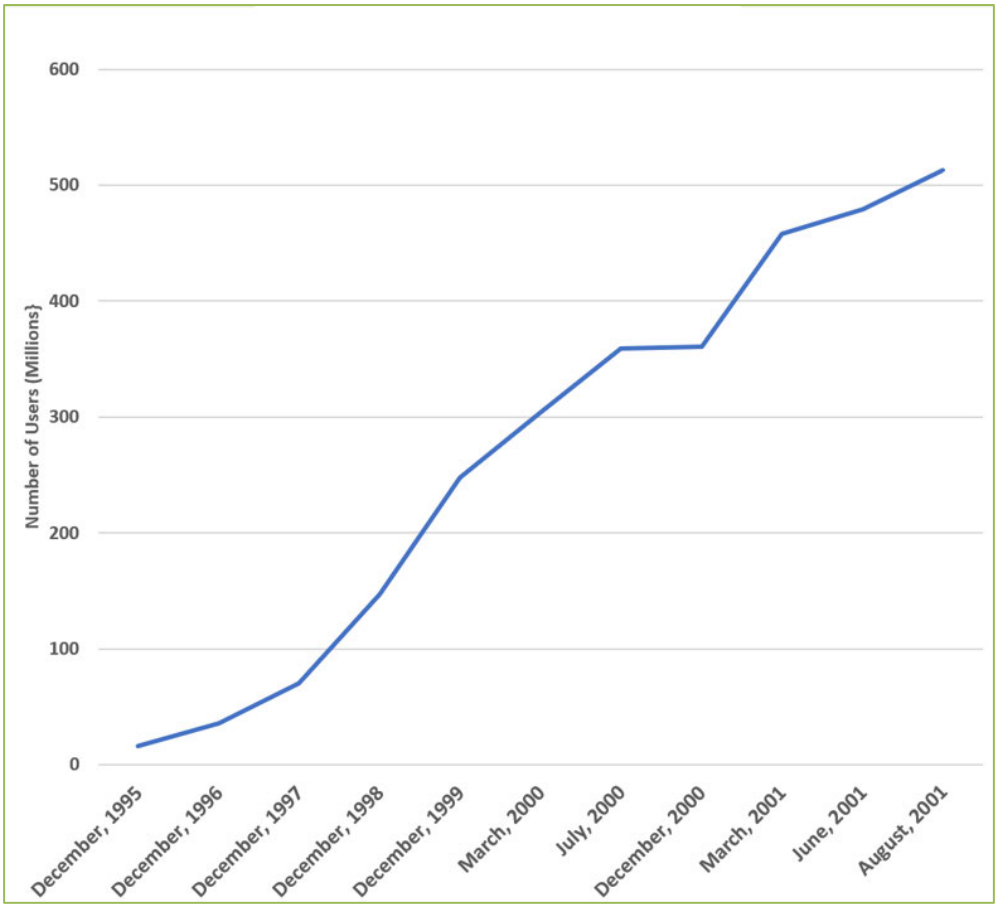


Figure 2.6. Internet growth history1995–2001 (adapted from Internet World Stats (2019))

In 1994 Kevin Poulsen, a computer hacker (and former phone phreaker), received a 51-month sentence for his part in scams that successfully defrauded radio station competitions, which was the largest sentence to be received by a computer hacker at the time (Brenner, 2010). In that same year, Dominic Rymer (a male nurse) hacked Arrowe Park Hospital's IBM mainframe and altered the details of several patients' prescriptions (Brenner, 2010). No deaths were recorded but the potential for cybercrime as a method of murder was realised (Brenner, 2010).

In 1998, Khan C. Smith extended David Dennis' 1974 idea (to disrupt end user terminals (as cited in Radware, 2017)) and demonstrated programming code that disrupted parts of the internet for over an hour (Smith, 2014). However, and crucially, samples of his code were released during a 'DEF Con' event (Kiyuna & Conyers, 2015), and these samples played a vital part in a much larger incident the following year (Smith, 2014), which saw Sprint, Earthlink (Credeur, 2002) and E-Trade (Sundar, 2017) all affected by a DDoS attack orchestrated by Michael Calce (Sundar, 2017).

Later, in 2000, Calce (then 15 years old) caused an estimated US$1.2 billion damage as he successfully impacted major companies such as Yahoo! and Amazon (Brenner, 2010; Kaspersky, 2016).

2.6 Organised Cybercrime

Up until 2006, efforts to cause disruption were typically done without malice, as the orchestrators were interested in the challenge of discovery and coveted the reward of notoriety; however, in late 2006, in response to political action taken by the Estonian Government, a DDoS attack was focused on an entire nation (McGuinness, 2017). In 2007, DDoS instigators demonstrated their ability to switch the internet on and off in Adygea and Astrakhan (Kaspersky, 2016), and it was at that point that DDoS attacks moved from largely simple personal discovery and fun to a way of inflicting tangible retaliation. The Estonian demonstration of control highlighted that these types of attacks could be strategically targeted, and it also highlighted the potential scale of the evolving threat. This realisation supported the development of an industry with a focus on cyber defence (Schmidt, 2016), and was a justifiable decision given the trend from the late 1990s which saw motivation move from bragging rights to organised disruption for personal and/or political gain (Campbell, 2018; Huntsman, 2019).

In March 2013, at least seven individuals (one Briton, one Dutch, two Americans, two Russians and one Chinese national (Jenkins, 2014)) formed a Russian-led group named Stophaus (Jenkins, 2014). These instigators were aggrieved with Spamhaus, an organisation that compiles and distributes DNS blacklists with the intent of reducing the amount of email spam. Spamhaus had detected and blacklisted botnet controllers that formed part of their cybercrime infrastructure. Spamhaus also went further, requesting that ISPs cut the internet connections of the companies hosting the criminal infrastructure (Krebs, 2013). In response, the group orchestrated a large DDoS attack (300 Gbps) aimed at Spamhaus's webservers, mail servers and name servers (Jenkins, 2014). Such was the scale of the attack, the London Internet Exchange (LINX) also experienced traffic congestion and reduced internet transport performance (Thomas, 2015).

Seth Nolan McDonagh, a 17-year-old British male who used the online pseudonym 'Narco' (Thomas, 2015), was arrested in April 2013 (Agence France-Presse, 2016).

He was charged with and admitted several offences and was finally sentenced in the British court in July 2015 to 240 hours of community service (Thomas, 2015). In another instance, 35-year-old Sven Olaf Kamphuis, a Dutch national (Tremlett, 2013), was arrested in Spain in April 2013 (Jenkins, 2014). In 2016, he was sentenced to 240 days jail; however, having already spend 55 days in jail prior to trial, the remaining 185 days were suspended by the judges, allowing Sven Olaf Kamphuis to walk from court (Agence France-Presse, 2016). These penalties are similar to those of Michael Calce, who under the pseudonym 'MafiaBoy' used DDoS in 1999 to impact Yahoo!, Dell, Fifa, Amazon, E*TRADE, eBay and CNN (CubCyber, 2020). For his crimes, which caused between US$7.5 million and $1.2 billion in damages, Calce received a small fine and eight months in open custody (CubCyber, 2020). These judgments appear to be highly lenient when compared to other penalties given for similar acts of organised crime. For example, in 2015, two Australian men were imprisoned for seven years and three months and three years and three months for their part in a AU$7 million insider trading scheme (Treasury Portfolio Ministers, 2015). Also, in 2021, an American CEO was sentenced to six years in prison for frauds that included a US$7 million COVID-19 pandemic loan fraud (Department of Justice, 2021).

2.7 Network Functionality

The existence of the modern-day internet relies on several stacked technology layers (Table 2.1) (Kabachinski, 2015). At the bottom (Layer 1) are the physical fibre, copper links and radio connections where wireless connectivity is achieved. Above this layer is the physical address of each network interface, commonly called MAC addresses (Media Access Control address; e.g., 00:1b:44:15:3c:d7) and above that is the IP address of the physical or virtual network interface, which is typically in either IPv4 or IPv6 format and is used for routing purposes.

Table 2.1

Protocol Stack

Layer ID	Layer type	Example use
7	Application	Data - HTTP, DNS
6	Presentation	Data - Data representation, Encryption, SSL, SSH
5	Session	Data – Sockets, ports, sessions, PPTP

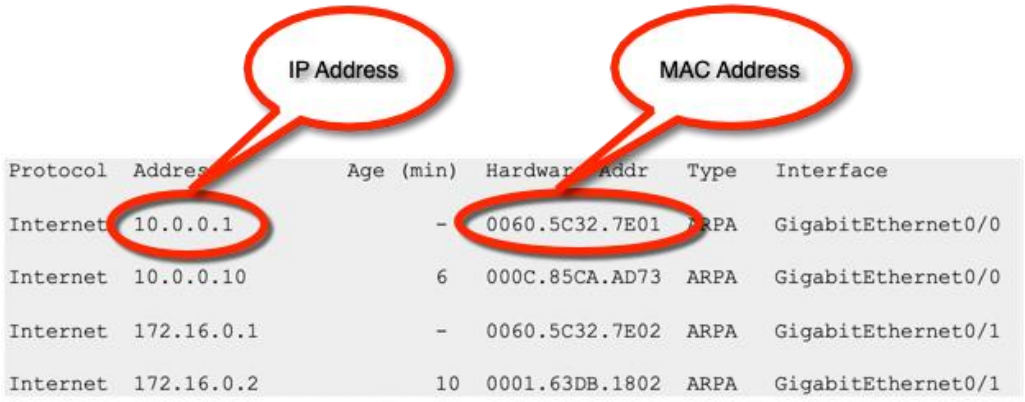
4	Transport	Segments - TCP, UDP
3	Network	Packets - Routing, IP, ARP
2	Data Link	Frames - MAC address
1	Physical	Bits - Transmission line, electrical signals

Note. Adapted from Kabachinski (2015).

IP addresses are important to networking as they provide a more readable format for an endpoint location. This IP to MAC address relationship is stored in each device's address resolution protocol (ARP) table, with the ARP table storing all the known MAC and IP addresses within the local or broadcast subnet. This ARP table (Table 2.2) is populated by an ARP broadcast process that queries all devices on the subnet to find which one has a particular IP address when the device is not already listed in the ARP table. The MAC address differs from the IP address in that the MAC address is somewhat permanently tied to a device whereas an IP address can be configured at will. A proportion of the MAC address is used to indicate the manufacturer. Using the example in Table 2.2, '**00:60:5C**:32:7E:01' would be from the manufacturer Cisco, and '**00:1b:44**:15:3c:d7' is a MAC address used by the SANDisk Corporation.

Table 2.2

Example ARP Table



This means that the remaining three hex numbers (e.g., 15:3c:d7) are able to give a manufacturer's device a somewhat unique ID. It is not necessarily completely unique, but the remaining IDs give a range of 00:00:00 to FF:FF:FF, which is over 1.6 million devices from a single manufacturer. While this is a limit, it is a limit that is unlikely to be realised as it is unlikely that 1.6 million devices would exist on a single private network.

However, IP addresses have the same limitation. Originally, IP addresses (IPv4) were made up of four octets written in the form of xxx.xxx.xxx.xxx. Each of the four octets has 8 bits, which in binary gives a range of 00000000 to 11111111. The common notation is written in decimal, which allows the range to be 0–255. Hence, the full range of an IPv4 address is from 0.0.0.0 to 255.255.255.255, which allows for 4,294,967,296 (2^{32}) individual addresses before any reserved ranges are removed. Even at just over four billion possible addresses, there are still not enough for each device in the world's population to be uniquely identified. According to Internet World Stats (2019), internet usage has surpassed 4.5 billion users, which has been driven by individuals having mutiple personal devices and the expansion of IoT (Priceonomics Data Studio, 2019). To combat this IP address limitation, IPv6 was released in 1998. This new version allows for 340 undecillion (2^{128}) unique addresses. For example, 8.8.8.8 is Google's IPv4 public DNS server address, and 2001:4860:4860:0000:0000:0000:0000:8888 (2001:4860:4860::8888 in short format) is Google's IPv6 address for the same service. IPv6 is more difficult to read and much more difficult to remember.

When a Uniform Resource Locator (URL) website address is typed into an internet browser, the DNS is the service that converts the readable URL into the less memorable IP address. The IP address provides a readable form of a device's network address and a form of alias that allows devices and computer systems to be replaced/maintained with minimal loss of connectivity. For example, if a DNS server points a domain address of www.example.com to an IP address of 192.168.1.1, an administrator could change the IP address record on the DNS server to a new server at 192.168.1.2 to allow maintenance to be performed without the users or systems of the readable address (www.example.com) being aware.

Similarly, attempting to access the URL dns.google.com would see a translation by the DNS into 8.8.8.8 or its IPv6 equivalent, which the underlying system would use as the address rather than the more human-friendly URL. The request follows the network stack down to Layer 1, where the electrical signals are transmitted to the next point on the path to their destination. Once the destination is reached, the data progress up the stack to the application layer, where the request is processed. Emails work in the same way, as the recipient's domain address must first be translated into an IP

address before routing can be attempted. With many systems utilising a readable URL rather than an IP address, the DNS has become a critical component of networking and the internet itself (Marrison, 2015). If name resolution fails, a large number of systems would be unable to communicate.

DYN.com is an internet domain registration and online infrastructure organisation that in 2016 hosted the name resolution for many large, well-known, global businesses such as Twitter, Reddit, GitHub, Amazon.com, Netflix and Spotify (Krebs, 2016). In October 2016, DYN were the subject of the largest DDoS attack incurred at that time. The attack at 1.2 Tbps (Novinson, 2018) involved tens of millions of IP addresses (York, 2016), and was made possible by infection with the Mirai botnet malware (Woolf, 2016; York, 2016) of some of the many devices and sensors that are connected to the public internet (commonly known as the Internet of Things (IoT)). In contrast to previous botnets constructed from infected PCs, Miria malware seeks to infect IoT devices such as security cameras, digital video recorders and baby monitors that have low security due to users installing with the default passwords in place (Cloudflare, 2019). Once installed, the malware deletes itself from the disk but remains active in memory until the unit is restarted. The Mirai botnet source code was made available through 'Hackforums' (an internet-based hacking community) in September 2016 (Manuel, 2018), shortly before the attack on DYN.

2.8 Internet of Things

The Internet of Things (IoT) is a term that describes the voluminous physical objects, devices, sensors and other technologies that connect and exchange data with other systems through the internet. According to Evans (2011), the term was derived from initial research at the Massachusetts Institute of Technology (MIT) but the Cisco technology company settled on it being the point in time where more devices than people were connected to the internet (Evans, 2011). The term therefore denotes a change in use. In the late 1990s to early 2000s, the internet was used by humans to access content created by other humans; however, humans began to access content generated by machine, and later machines began to communicate with other machines (Song et al., 2017). Due to this shift, Cisco has identified the birth of IoT as being somewhere between 2008 and 2009 (Evans, 2011). In order to illustrate the benefits

of IoT in a real-world example, one common model is the relatively recent development of smart cities (Song et al., 2017). Smart cities use multiple sensors to collect and record data that can then be used to manage the various resources, assets and services as efficiently as possible (Figure 2.7).

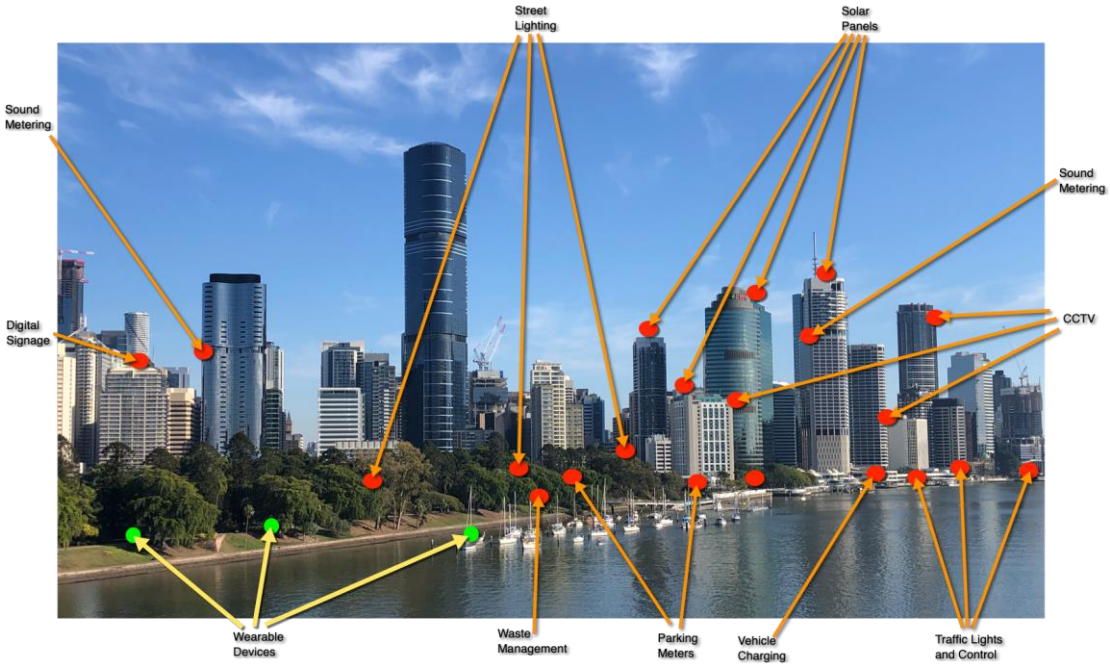


Figure 2.7. Smart city sensors (by researcher)

Communicating through the public internet, either openly or via virtual private networks (VPN), sensors can be used to detect current daylight, quantity of pedestrians and available stored solar power in order to determine the most efficient use of street lighting, digital signage and traffic control. The advantages are increased clarity and a deeper understanding and automation of responses; however, there are also additional risks. Control systems such as those used for water distribution and treatment are developed with a focus on functionality rather than security (Song et al., 2017). Traditionally, these systems would have been safely behind security perimeters of closed networks with little need for cyber defence; however, the introduction of IoT to initiate the automated responses gives would-be attackers easy access to these control networks. Once connected, attackers can capture sensitive information, manipulate data or, as demonstrated by Vitek Boden who released 24,000 gallons of sewage into a river, physical infrastructure can be controlled and used to cause incidents that affect the public at large (Sayfayn & Madnick, 2017).

IoT devices in smart cities have access to connectivity from the widely available internet copper and fibre cables as well as wireless and 4G/5G networks. In more remote areas, therefore, there are potential connectivity issues with IoT devices as well as corresponding security challenges. As remote areas often do not have the same plentiful level of network infrastructure as cities, IoT devices make use of other options such as the LoRa (long range) network protocol (Butun et al., 2021) and other LPWAN (low power wide area network) technologies (Torres et al., 2021). While DDoS is commonly considered to be an attack that originates at a remote location and travels through the target's internet gateway (Figure 2.8), these IoT devices present an alternate attack vector.

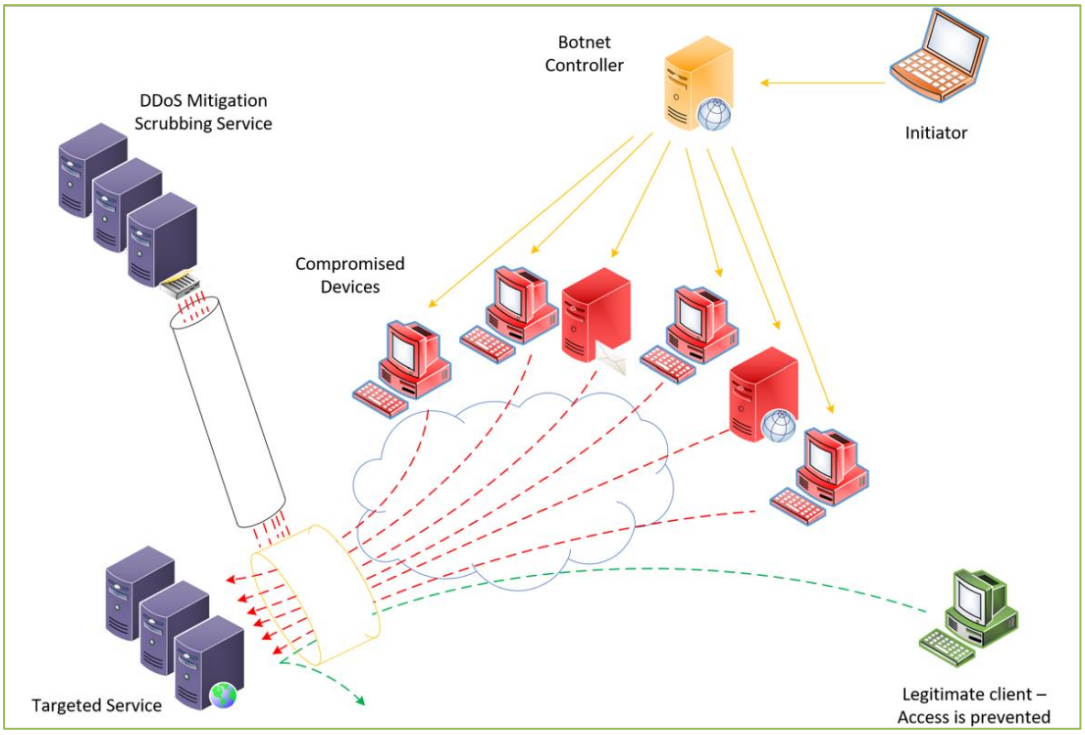


Figure 2.8. Common DDoS entry from internet (by researcher)

For example, as shown in Figure 2.9, an initiator who is outside of a building but is in close proximity to a compromisable wireless device may be able to construct a DDoS logically from the inside of what was thought to be a protected network by compromising one or a series of IoT devices. While an organisation's internet gateway may have layers of detection, mitigation, hardware and software, they are generally focused on incoming traffic, and all the protective technology would be redundant if the DDoS attack traffic reached its target without traversing the monitored networks. Therefore, a DDoS initiated from inside the secure perimeter could easily target

critical network paths or subsystems and take systems offline with less brute force or sophistication than externally generated attacks.

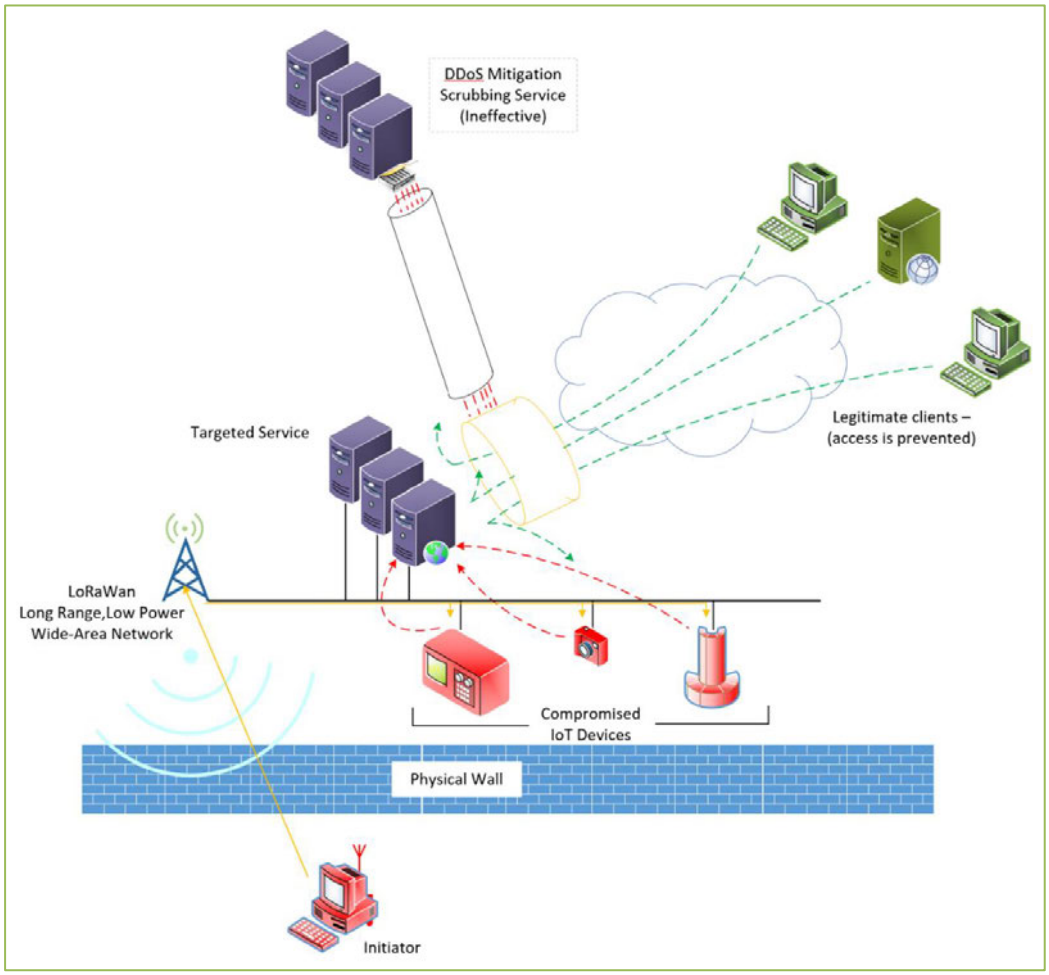


Figure 2.9. Less common DDoS initiated from inside (by researcher)

2.9 DDoS at Scale

A report by Netscout highlighted recent attacks that reached a peak of 800 Gbps (Anstee et al., 2017), but the attack on DYN and a later attack on GitHub (a cloud-based software repository and versioning platform) at a magnitude of 1.3 Tbps in February 2018 (Ghoshal, 2018) eclipsed the volumetric record. GitHub had somewhere between 24 and 31 million users at the time (GitHub, 2018; Swift, 2017), which is comparable to the population of Australia. Robert Graham reports that the attack on GitHub was probably orchestrated by the Chinese Government (as cited in Graham, 2015). Using a customised traceroute script, Robert Graham was able to detect where a man-in-the-middle (MITM) device was positioned in the network. This

MITM device was situated on or near the Great Firewall of China (a subsystem of China's Golden Shield Project (Wu & Lam, 2017)), which uses IP blocking, DNS hijacking and keyword inspection/filtering to enforce internet filtering and censorship for Chinese residents (China Correspondent, 2013). The MITM device forms part of an infamous DDoS tool called The Great Cannon (Cimpanu, 2019a), and it intercepted requests that were heading to Baidu analytics (China's version of Google Analytics (Li, 2016)) and replaced the content with JavaScript code that was written to attack GitHub (Graham, 2015). When an individual outside of China accessed the Baidu Analytics site to collect their website statistics, they inadvertently executed the JavaScript code, which led to a globally distributed DoS attack (Graham, 2015).

As can be seen in Figure 2.10, there was substantial volumetric capacity growth in DDoS between 2010 and 2020, with 2017–2018 demonstrating faster DDoS volume growth than the internet itself (approx. 60% of the world population (Internet World Stats, 2019)).

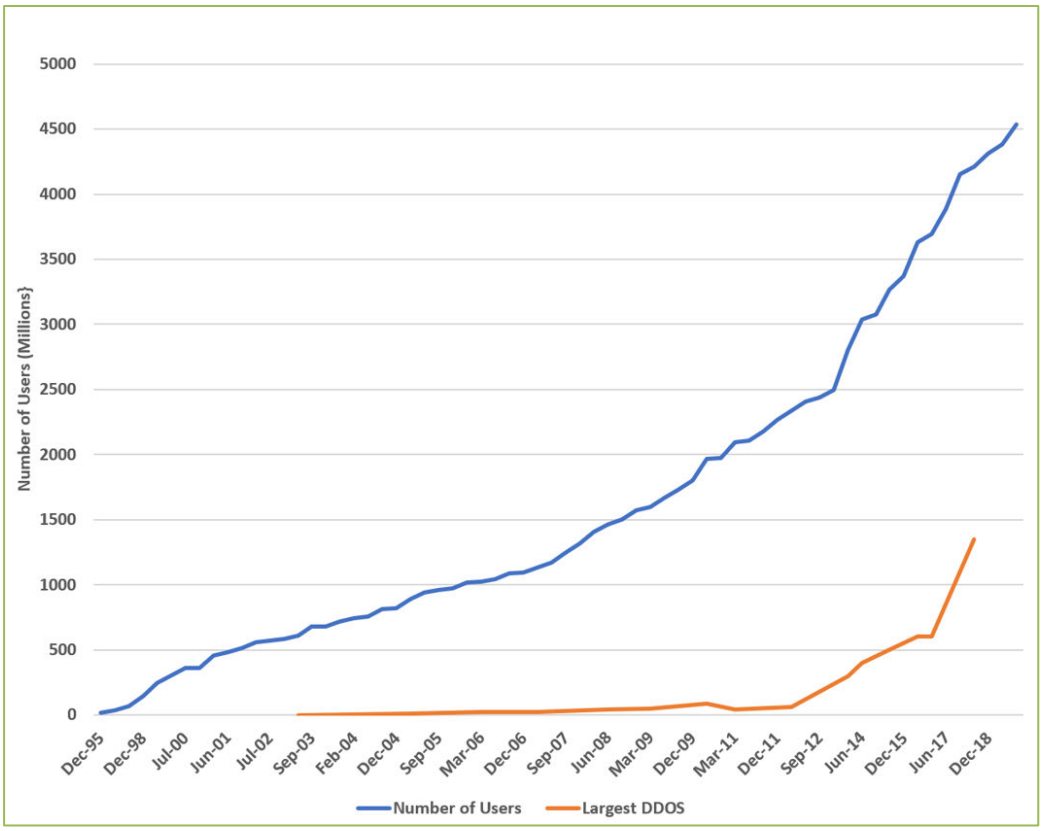


Figure 2.10. DDoS attack volume and internet usage 1995–2019 (compiled from Anstee et al. (2017) & Radware (2017))

The scale and frequency of these types of events continued to increase through to 2019 (ACSM_Admin, 2019; Campbell, 2018). In 2019, Kaspersky reported the discovery of a new version of the Mirai botnet code (Kupreev, Badovskaya, & Gutnikov, 2019a). This new code expanded the potential compromisable targets to include wireless presentation devices and digital signage (Kupreev, Badovskaya, & Gutn, 2019a). This expansion increased the potential for larger volume attacks in the future and indicates that a continued rise is likely.

However, a small reduction in global attack of resources occurred in January 2019 with four legal convictions occurring.

1. The US Department of Justice seized 15 internet domains that it claimed had been used to perform DDoS attacks on government systems, universities, gaming platforms, financial organisations and ISPs across the world (Kupreev, Badovskaya, & Gutnikov, 2019a).
2. A US court jailed a 34-year-old Massachusetts hacker (Martin Gottesfield) (Cimpanu, 2019a; Wolff, 2019) for 10 years for launching the DDoS attacks on two medical facilities, one of which was the Boston Children's Hospital, as he protested the psychiatric detention of Justina Pelletier (Wolff, 2019).
3. British police arrested 32-year-old Daniel Kaye who built a Miria botnet from hacked Dahua security cameras and other devices that he rented from other hackers (Daws, 2019). Kaye had been hired by a senior official at competitor Cellcom to ruin the reputation of Lonestar (a Liberian telco) (Daws, 2019).
4. A total of 250 cyber criminals were arrested in Britain and the Netherlands by Europol (the European Union's law enforcement agency) following the 2018 shutdown of Webstresser.org (Krebs, 2019). In a slight change to other previous prosecutions, the investigation was not limited to the criminals who orchestrated the attacks, and further investigation into the 150,000 clients (worldwide) who used the service is underway (Krebs, 2019; Kupreev, Badovskaya, & Gutn, 2019a).

However, this public display of justice did not dissuade the criminal fraternity from undertaking further attacks. Several large and obstructive DDoS attacks were recorded throughout 2018 and beyond.

- February 2018 – GitHub 1.3 Tbps (Ghoshal, 2018).

- March 2018 – Netscout record a 1.7 Tbps memcached reflection/amplification attack on one of its customers but did not provide the name of the target.
- February 2019 – The National Union of Journalists of the Philippines was the target of a 468 Gbps DDoS attack (Kupreev, Badovskaya, & Gutnikov, 2019a).
- March 2019 – A DDoS attack was used to target a computer system that regulates the supply of electricity to various districts of Los Angeles and Salt Lake City. Additionally, as a consequence, power supply systems in California and Wyoming also experienced problems (Fazzini & DiChristopher, 2019).
- April 2019 – In response to the UK arrest of Julian Assange that followed his asylum revocation, Ecuadorian facilities became the target of a very large number of cyber-attacks, including DDoS. These attacks targeted the websites of the Central Bank, the Ministry of Foreign Affairs and the Presidential Office (Dan, 2019). To cope with the onslaught of digital indignation, Ecuador had to seek help from Israeli experts (Kupreev, Badovskaya, & Gutnikov, 2019b).
- June 2019 – Telegram, an encrypted cloud-based instant messaging service, was attacked with a DDoS where the source consisted primarily of Chinese IP addresses (Porter, 2019). Founder, Pavel Durov, believed Hong Kong demonstrations were the motivation as the political opposition used Telegram to securely organise protests (Kupreev, Badovskaya, & Gutnikov, 2019b).
- August 2019 – Similar to the attack on Telegram two months prior, China used The Great Cannon to launch an attack on the LIHKG Forum (Cimpanu, 2019a), as it was a key website used by protesters to coordinate their actions in Hong Kong (Kupreev, Badovskaya, & Gutnikov, 2019c). The forum owners reported that 1.5 billion requests were received in 16 hours (average 26,000 rps), causing a temporary outage and the malfunction of their mobile app (Kupreev, Badovskaya, & Gutnikov, 2019c).
- September 2019 – Wikipedia became temporarily unavailable to users in several countries (Europe, Africa and the Middle East) (Kupreev, Badovskaya, & Gutnikov, 2019c). Unofficial sources report the volume of the attack at greater than 1 Tbps over the three-day duration (Kupreev, Badovskaya, & Gutnikov, 2019c).

- February 2020 – AWS reported a new record in DDoS capacity. Aimed at Connectionless Lightweight Directory Access Protocol (CLDAP) web servers, the volume reached 2.3 Tbps, which was higher than the previous record of 1.7 Tbps recorded in March 2018 (Nicholson, 2020).
- November 2021 – Cloudflare reported a short but intense DDoS attack of just under 2 Tbps that combined UDP flooding and DNS amplification generated by a botnet of approximately 15,000 IoT devices and unpatched GitLab instances.

The statistics presented in Figure 2.11 confirm that the capacity and frequency of attacks are increasing (Mansfield-Devine, 2015; Nazario, 2008); however, a third attribute of DDoS is also advancing.

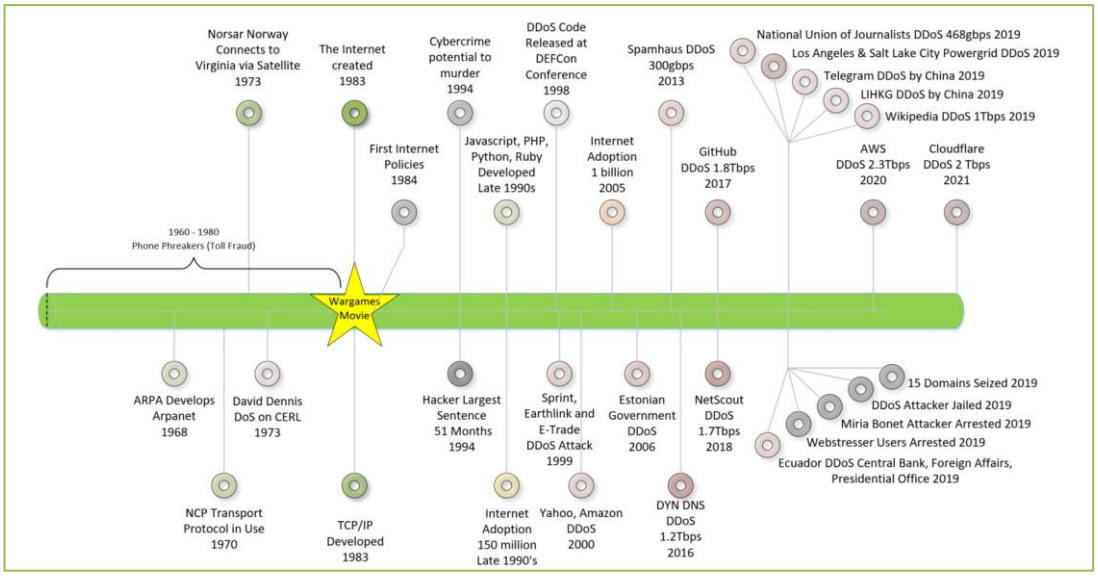


Figure 2.11. Event timelines (compiled from Adams et al. (2006); Anstee et al. (2017); Atwood (2006); Brenner (2010); Ghoshal (2018); Jenkins (2014); Kiyuna et al. (2015); Kizza (2017); Krebs (2016); Kupreev et al. (2019a, 2019b, 2019c); McGuinness (2017); Nicholson (2020); Norsar (2016); Radware (2017); Schulte (2008); Smith (2014); Sundar (2017); The White House (1984))

As protective measures achieve mitigation capability, DDoS attacks are increasing their sophistication and complexity. Where initial attacks were aimed at flooding a network pipe with traffic (thus preventing legitimate traffic from reaching its destination), later forms have become more targeted and now seek to disrupt the vulnerable areas of a supplied service by amplification methods or service exhaustion

inside of software capability (Pitlik, 2019; Wueest, 2014). For example, a SYN-ACK approach (Figure 2.12) relies on the fact that there are a limited number of unique ports available to a server (Cybersecurity and Infrastructure Security Agency [CISA], 2009).

2.10 Forms of Attack

Other forms of attack can be described by commonly accepted terminology and fall into three primary categories: volume based, protocol based and application based. While each of these has a specific target type and method, they all may benefit from amplification methods, so each has an additional 'amplification' subcategory.

2.10.1 Volume-based Attacks

Infrastructure layer attacks that are focused on layers 3 and 4 (network and transport layers) are the most common, mainly due to their simplicity. These volume-based attack types include User Datagram Protocol (UDP) floods, Internet Control Message Protocol (ICMP) floods (ping floods) and Domain Name System (DNS) floods (Walkowski, 2019). On the path to a server, each network device and network link along the route has a maximum amount of data that it can cope with. The capacity of these devices and links is measured in a multiple of bits per second (bps), such as 1 Gbps for a typical wired LAN or 40 Gbps for a server connection. Once capacity is full, any data sent along this path will fail to deliver when it reaches the congested point. Therefore, the goal of this type of attack is to overwhelm the available bandwidth connecting the targeted site or the capacity of the server. The attacker simply has to generate enough data to overwhelm the capacity link of the smallest device along the network route. The 2020 DDoS of AWS at 2.3 Tbps easily eclipses the 400 Gbps capacity of a very large internet connection; however, it is currently less than the fastest internet connection in development as of 2020 (at 44.2 Tbps) (Monash University, 2020).

UDP flood

UDP and TCP are protocols that both transmit data via an IP network; however, they have a major difference, which is that while the TCP requires a handshake process before data is exchanged, the UDP does not. This means that the TCP is ideal for situations where error correction is required and where large amounts of data (that are

segmented for sending) need to be reassembled in the correct order on receipt. The TCP handshake, commonly referred to as SYN-ACK, relies on a three-step process that a client and server uses to establish a connection (Figure 2.12). It is an important step that occurs prior to any real data transfer as it ensures both ends are ready to conduct the transfer.

- The first step is where the **client** sends the server a SYN (synchronise) packet with an initial sequence number and waits for a reply.
- On receipt of the SYN packet, step 2 sees the **server** chooses its own initial sequence number and responds with a SYN-ACK (synchronise-acknowledge) packet which contains its own sequence number and an acknowledgment of receiving the client's sequence number in the form of the client's number incremented by one. The server then waits for a reply.
- The client receives the SYN-ACK packet, performs the final step and sends the **server** an ACK (acknowledge) packet which contains the servers sequence number (incremented by one).

With the final step complete, a socket connection is established, and two-way (full duplex) data transfer can begin.

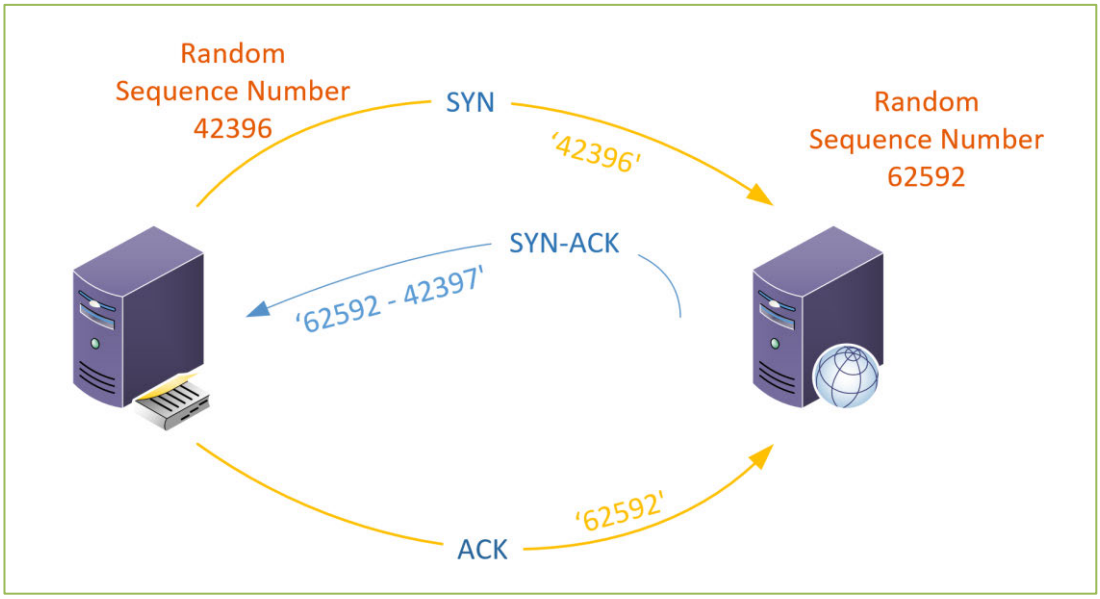


Figure 2.12. TCP 3-way handshake process (by researcher)

In contrast, the UDP has no handshake requirement. It is utilised where no receipt of delivery is required and receipt of data is taken on an as-delivered basis even if out of

order. This makes the UDP an ideal protocol for broadcasts and multicasts; however, due to its simplicity and packet structure, it is also used for DNS, DHCP, NTP and SNMP. These UDP requests include a port number that usually aligns with one of the well-known standard port allocations (e.g., port 53 for DNS or port 123 for NTP) (Internet Assigned Numbers Authority [IANA], 2020). In a UDP flood attack, the target system is sent multiple UDP packets, each with a random port assigned (Figure 2.13).

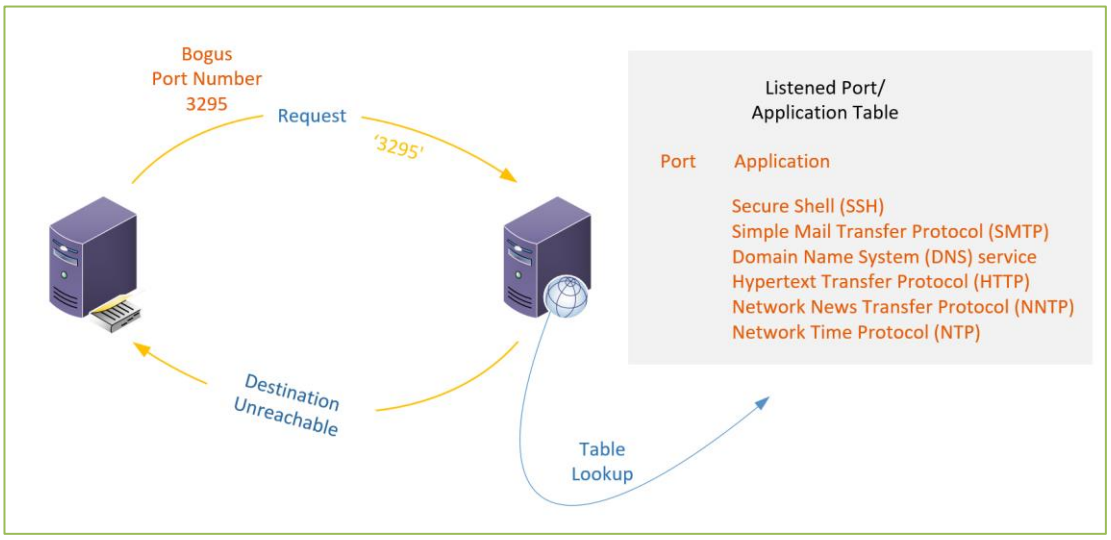


Figure 2.13. UDP flood attack (by researcher)

-

When the packet arrives, the target system searches for an application assigned to listen on that port. If no application is found, the target system replies with a 'destination unreachable' packet and the target system's time is wasted. If too many random requests are received, the target system repeatedly searches for listening applications, which causes resource depletion and the system becomes unreachable as it is unable to respond to legitimate requests.

ICMP (ping) flood

ICMP or ping flood attacks do not use UDP or TCP but instead rely on a type 8 (echo message) or type 0 (echo reply message) being sent across ICMP. There are just less than 50 types of ICMP parameter, of which a ping uses two (IANA, 2018). A ping requires no ports to be assigned as the ping command is used to verify the communication between two system endpoints. The default request size of a ping is 32 bytes for Windows operating systems and 56 bytes for a Linux operating system;

however, this can be increased to 65.5 kB when the -l option is used (e.g., ping 151.101.0.81 -l 65500).

When the target system receives a type 8 (echo message). It responds with a type 0 (echo reply message). Essentially, if the attacker has access to more bandwidth than the target, the attack will be a success as if enough requests are sent (without waiting for a reply), the target system may be overwhelmed and become unreachable. With modern day networks, this is an unlikely occurrence as a standard 1 Gbps network connection could cope with almost one million 64 B ping requests per second. In addition, perimeter networks can be configured to drop ping requests that originate from outside of the organisation's network or to set limits for the size of ping requests. The calculation in Figure 2.14 adds a division by two in order to accommodate the assumed capacity for each additional reply.

1 Gbps link = 125,000,000 Bps

(125,000,000 Bps ÷ 64 B) ÷ 2 = 976,562.5 (pings per second)

Figure 2.14. Number of pings for a 1 Gbps link

DNS flood

In a DNS flood, an attacker sends a large number of DNS requests to the target's DNS server. The DNS server first checks its DNS cache to see if it has been recently resolved. It then checks the authoritative server to get the IP address (Figure 2.15).

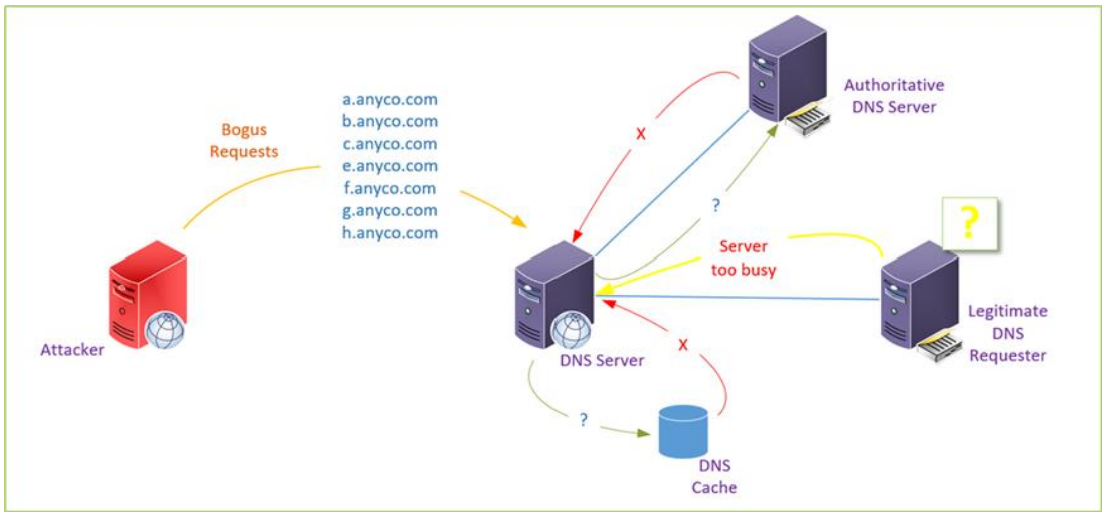


Figure 2.15. DNS flood attack (by researcher)

As the request is for a bogus address, no corresponding IP address will be found and the request has used up valuable resources while it attempts to serve the bogus request. As the DNS server is unable to distinguish between legitimate and hoax requests, it attempts to respond to all requests and may eventually be overwhelmed with the effect that any services that require legitimate DNS resolution become unable to get their request through and, consequently, those services also begin to fail.

2.10.2 Volume-based Attacks – with Amplification

While volume-based attacks seek to overwhelm their target's bandwidth with the data they send and receive, with amplification, the attacker makes use of the lack of symmetry between request and reply that some requests can generate. A ping request acts with a 1:1 ratio, thus when 32 bytes are sent, 32 bytes are received. However, other requests may generate a much larger response from a simple request such as the Network Time Protocol (NTP) request explained below.

NTP amplification attack

In NTP amplification attacks, the perpetrator exploits publicly accessible NTP servers to overwhelm a targeted server with UDP traffic. By sending a 'get monlist' request to an NTP server, the server responds with a reply that is many times the scale of the original request. It is therefore defined as an amplification attack as the query-to-response ratio could be between 1:20 and 1:200 the size of the original request. By spoofing the source IP address, the attacker can send this amplified traffic response to the target server address (Figure 2.16).

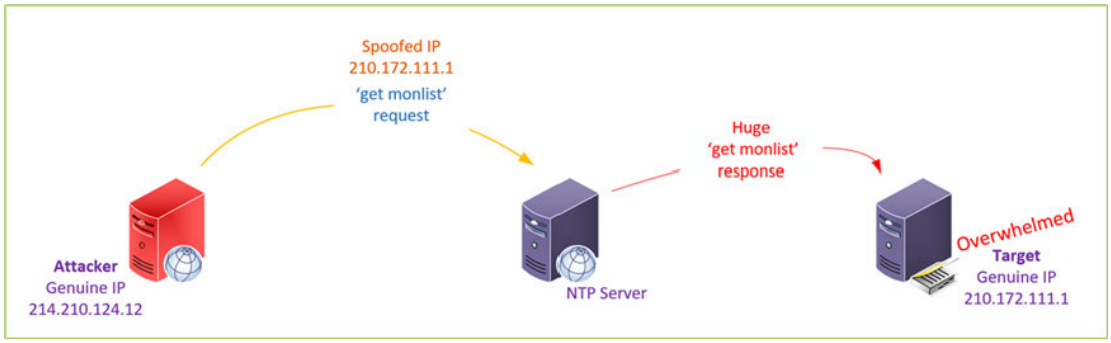


Figure 2.16. NTP amplification attack (by researcher)

-

Ultimately, this means that any attacker who obtains a list of open NTP servers (which is easily obtained via a simple Google search) can easily generate a high-bandwidth and high-volume DDoS attack.

DNS-reflected amplification attack

Unlike a DNS flood where the victim's own DNS server is flooded with fake requests, in a DNS-reflected amplification attack, malicious actors use publicly accessible ("open") DNS resolvers to flood a victim's system with fake DNS responses. This works in a similar way to an NTP amplification attack except that the attacker sends DNS lookup requests to these open DNS resolvers, thus spoofing the source IP address to that of the target. Because the requests appear to come from the target, the DNS resolvers (acting as reflectors) send all responses to the target's system instead of the attacker's, even though the victim never made any requests. This is referred to as an amplification attack as the size of the DNS response is much larger than the size of the request. As shown in Figure 2.17, a query that uses the type 'any' is requesting that a DNS server return to the target's system all records known to contain the queried value. This means that a single 120byte DNS query sent to a DNS server could generate a 500byte response. Therefore, the volume of the response this generates can overwhelm the target, rendering it unable to respond to legitimate requests and effectively taking it offline.

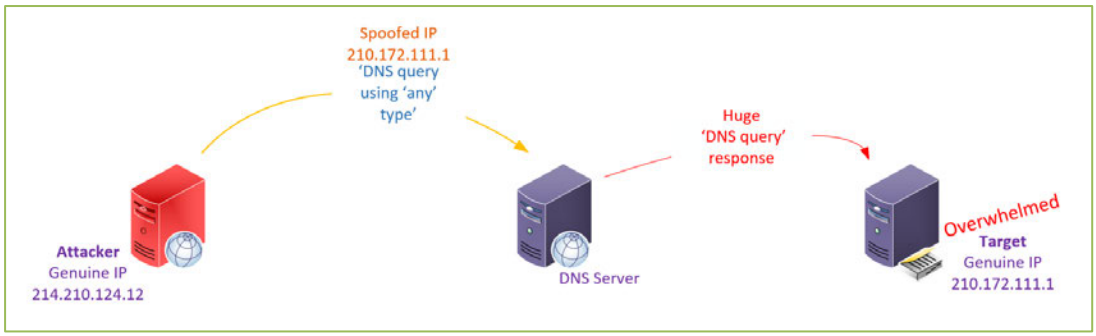


Figure 2.17. DNS amplification attack (by researcher)

-

Smurf attack

In a Smurf attack, the attacker sends ICMP (ping) broadcast packets to a number of hosts with a spoofed source IP address that belongs to the target machine. The

recipients of the packets will then respond but the responses will be directed to the target's IP address and the target will be flooded with those responses (Figure 2.18).

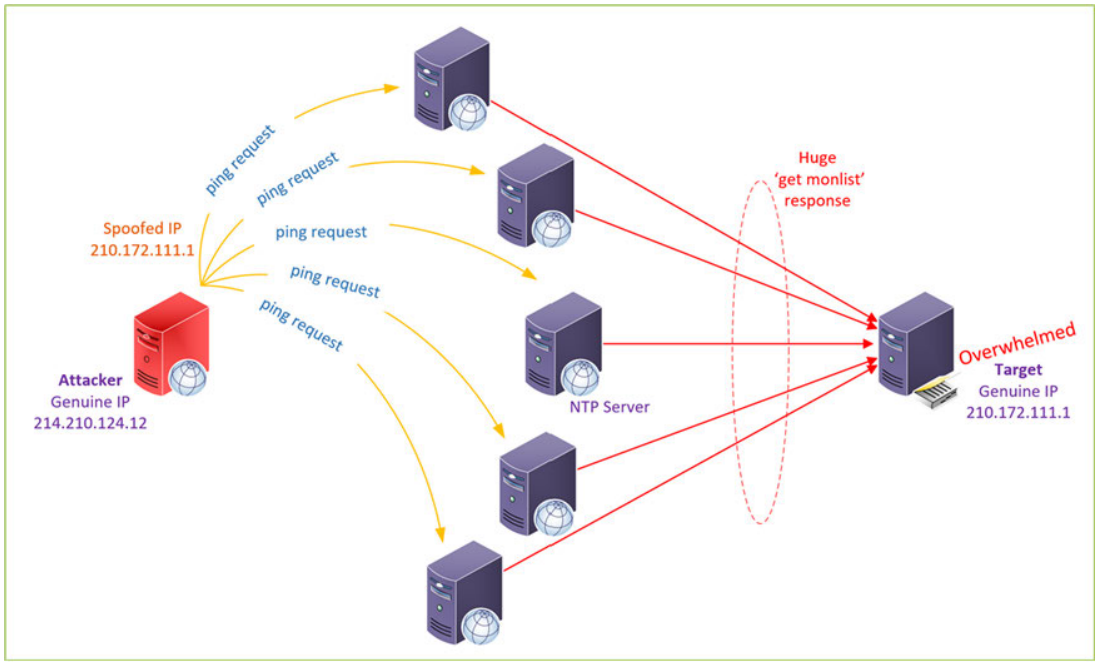


Figure 2.18. Smurf attack (by researcher)

2.10.3 Protocol Attacks

In contrast to the volumetric attacks that target the bandwidth of the target, protocol attacks exploit protocol mechanisms in order to consume system resources. These types of attack are not just limited to consuming the targeted servers' resources, but may also consume the resources of any intermediate communications equipment encountered along the route, such as firewalls or load-balancers, as part of the attack strategy. Whereas volumetric attacks are measured in bps, protocol attacks are generally measured in packets per second (Pps).

Ping of death

The ping of death (PoD) attack is more complex than simply sending a mass of ping requests to a server. The PoD relies on the maximum frame size (maximum transmission unit – MTU) of the data link layer, which commonly has a maximum of 1,500 bytes compared to the maximum packet size of a ping request at 65,535 bytes. Sending a ping of over 1,500 bytes requires the packets to be split into multiple

fragments smaller than the 1,500 bytes (MTU) and sent individually. On receipt, these multiple fragments are reassembled into the original packet and the ping is executed (Figure 2.19).

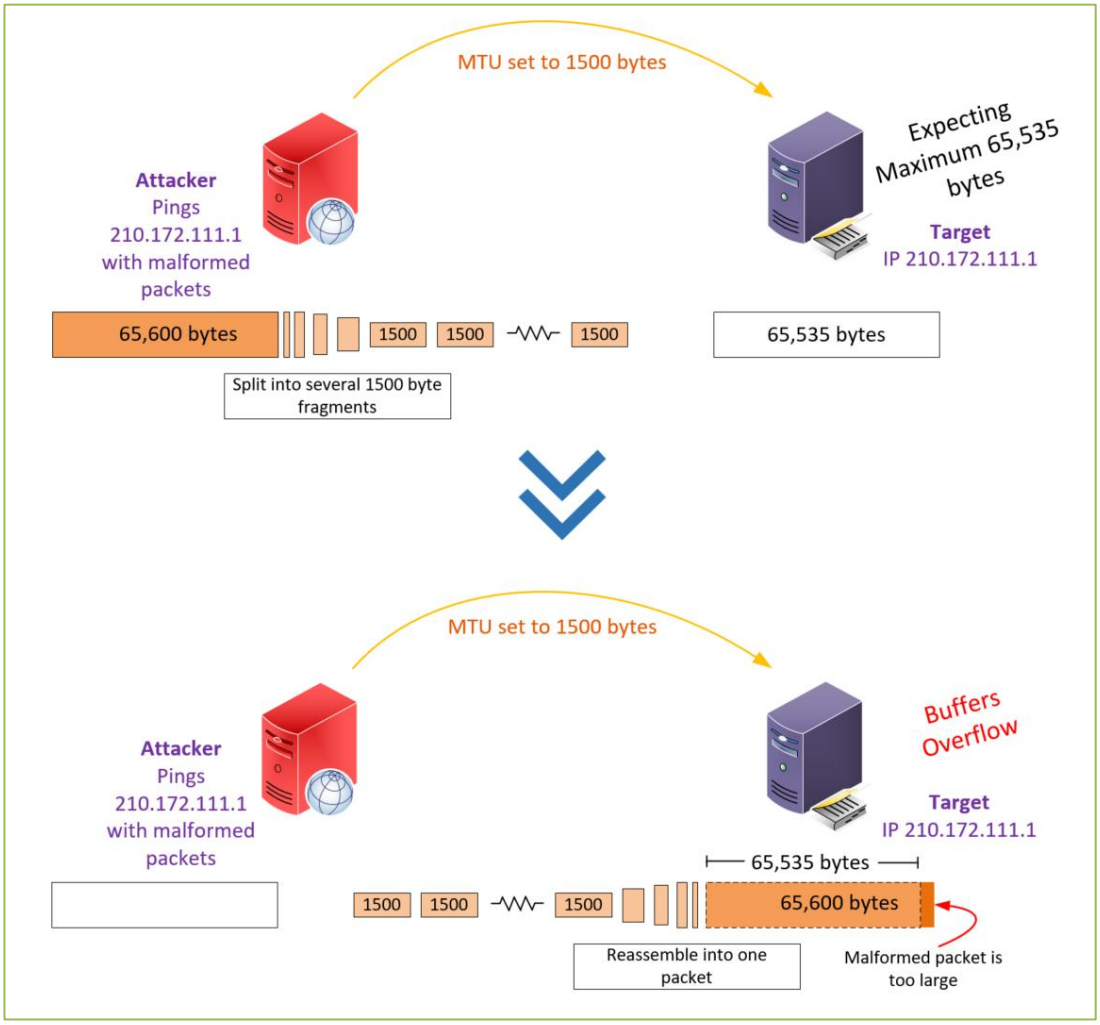


Figure 2.19. Ping of death (by researcher)

As illustrated in Figure 2.19, a PoD can occur when an attacker maliciously manipulates the fragment content causing the recipient to receive an IP packet that is greater than 65,535 bytes when reassembled. This leads to buffer memory overflow, which in turn prevents the acceptance of legitimate packets and may cause a system to crash (Abdollahi & Fathi, 2020). Legitimate packets are denied service and the PoD has succeeded (Buffered, 2018). Although Microsoft and Linux distributors have previously released patches for their operating systems relating to this attack type, it still periodically gets referred to in later updates (Varghese, 2019).

SYN flood

A SYN flood attack uses the process that underpins the successful establishment of a TCP connection required prior to data transfer. When a data transfer is requested, the TCP initiates a connection using a process referred to as the TCP 3-way handshake (Figure 2.12) (Antoniou, 2009).

A SYN flood attack utilises the period where the target is waiting for a response, as until the response is received, the connection (port) is held open. As network transmissions can be unreliable, there is a (configurable) timeout after which a port is returned to the pool of available connections, but the pool is limited, and the timeout can be quite long. In a SYN flood attack (Figure 2.20), the requester either sends the target a SYN request with a spoofed source IP or they send the SYN request then refuse to answer the return SYN-ACK. Either way, the target's available connections are consumed, preventing legitimate access (CISA, 2009). A server may, for example have 13,000 available connections with a timeout period set to 240 seconds, which allows an average of 54 connections per second. If enough spoofed SYN packets are sent to a server, all of its available ports could be held open for the timeout period and all connections may be waiting for an ACK response. The server is effectively disconnected, as no new connections are possible. Therefore, a service may be disrupted with a relatively small amount of originating traffic.

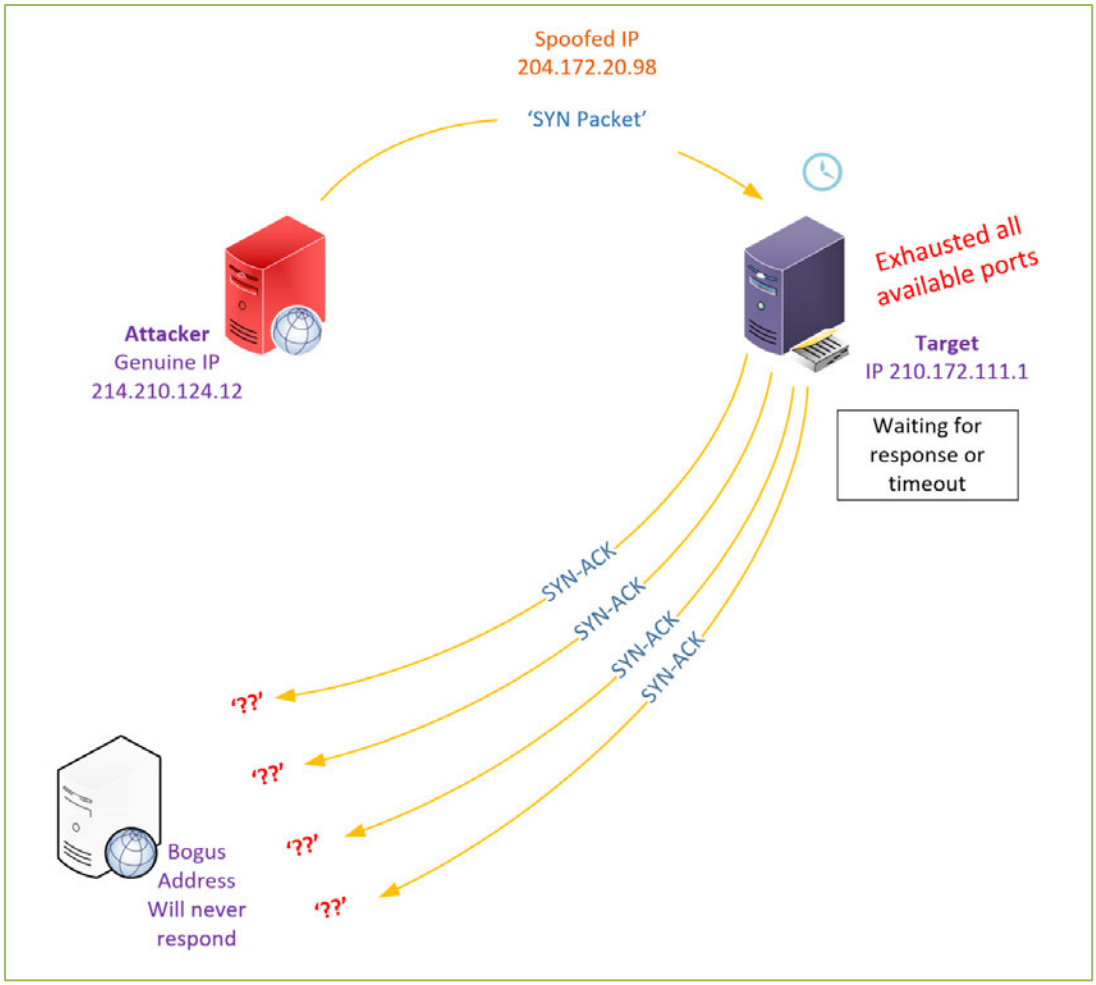


Figure 2.20. SYN flood attack (by researcher)

TCP middlebox reflection

Bock et al. (2021) discuss a new form of amplified DDoS attack that uses a failure of network middleboxes to be TCP compliant. Middleboxes are network devices that are in the network path and perform functions other than packet forwarding, such as intrusion dectection, intrusion prevention, firewall proxies and network optimisers (Sherry, 2015). In some cases, middleboxes are required to inject packets so they can perfom censoring functionality; however, due to the asymmetric routes in the internet, the middleboxes may not see the entire TCP connection. As such, they can be configured in a non-TCP compliant way, thus allowing them to block connections even when the entire packet stream has not been received. Because of this non-compliance, Bock et al. (2021) found that it would be possible to convince a middlebox that a TCP handshake had occurred, and cause them to deliver a block pages response that can be quite large and hence deliver a very large amplication factor. CDN vendor Akamai claim to have detected waves of attacks, which highlights

that this method has moved from a researched possibility to practical use by attackers (Tung, 2022).

2.10.4 Application Layer Attacks

Application layer attacks focus on layers 6 and 7 of the protocol stack. They work by exploiting resource-expensive requests and queries and tying up resources, which renders applications unavailable to legitimate users. For example, a request through an application programming interface (API) to retrieve 1 million database records using a complex query would allow a small request to generate a massive load on the server. Consequently, these types of attack are often smaller in volume, which makes them more difficult to detect, but they can be equally as disruptive as other forms of attack.

Slowloris

A Slowloris attack is a highly targeted form of attack that allows a server to affect the performance of a web server. Crucially, it does this without affecting other services or ports on the target network. It is performed by holding open many connections to the target web server as possible for as long as possible (Figure 2.21).

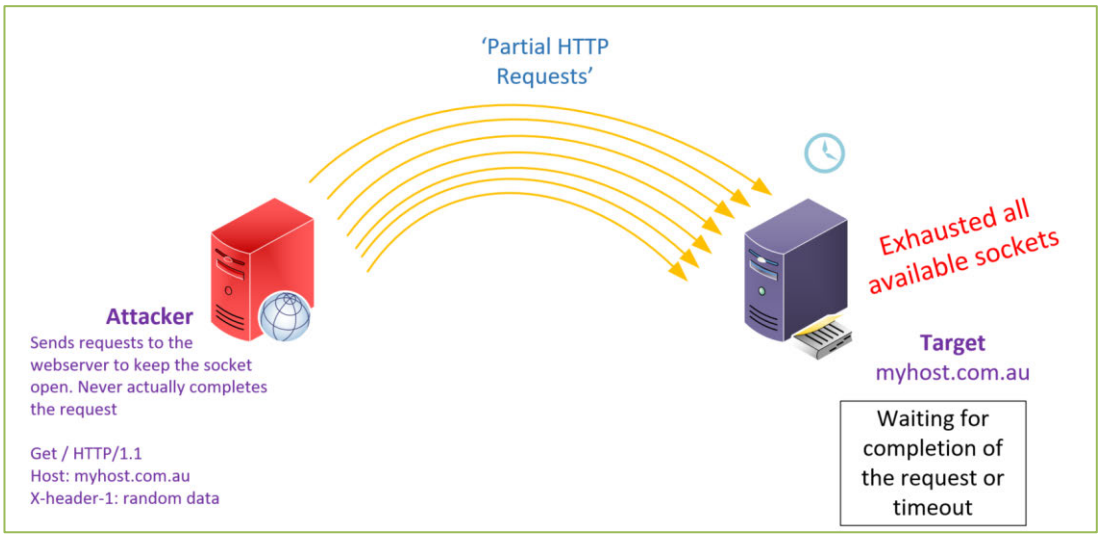


Figure 2.21. Slowloris (by researcher)

The initiating webserver creates connections to the target web server (Figure 2.22) but only sends partial requests. It then continually sends more and more Hypertext Transfer Protocol (HTTP) headers without completion and because of the mass of open bogus connections, the targeted server exhausts its concurrent connection pool,

which leads to the denial of additional connections from legitimate clients (Walkowski, 2019).

HTTP flood

HTTP flood attacks use HTTP GET or HTTP POST requests to attack a web server or application by seeking to consume resources through the process of issuing malicious requests (Figure 2.22). Typically, POST requests are more computationally expensive than GET requests, as POST requests relate to dynamic content while GET requests relate to static content. HTTP flood attacks seek to exhaust the resources of the target web server, rendering it unable to service legitimate requests. As this form of attack does not use malformed packets and is often initiated from distributed botnets, it is very difficult to detect and that detection may rely on processes known as source IP reputational analysis (Technology Org, 2018)

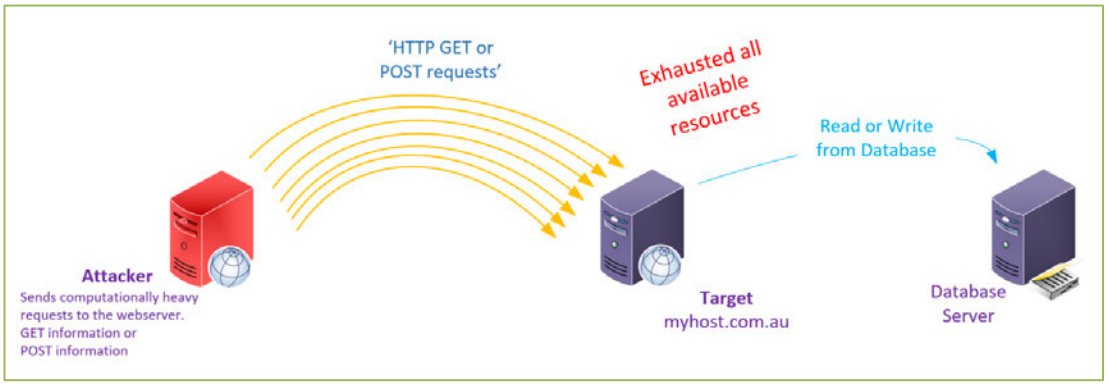


Figure 2.22. HTTP flood (inc cache bypass) (by researcher)

HTTP flood–cache bypass

An HTTP flood–cache bypass attack (Figure 2.23) works in a similar way to HTTP flood but there is a subtle difference in that the type of data requested is data that cannot be cached. This is intended to consume maximum resources as the server needs to request data from the source rather than the much closer and computationally cheaper cache memory (Gopalan, 2019). Like HTTP flood, this type of attack is also easily hidden as it does not use malformed packets, can include requests for commonly searched themes such as “gov” or “news” and can request dynamic data. Essentially, they appear to be legitimate use (Sucuri, 2019).

Heavy URL

As another highly targeted attack, the heavy URL (Figure 2.23) seeks to exploit the most resource-costly URLs on the target server. However, this form of attack requires advanced knowledge of the target. During investigation, the attacker identifies which of the target URLs require the most computational effort, such as intense and complex database queries. The attacker then performs these queries en masse to establish a DDoS attack – in other words a biggest "bang for buck" approach. While the attacker's HTTP requests are relatively small, the outcome for the target can be exhaustive as it may have to process large files or perform complex and recursive database queries. Once the target's resources are exhausted, legitimate access is denied service (Walkowski, 2019).

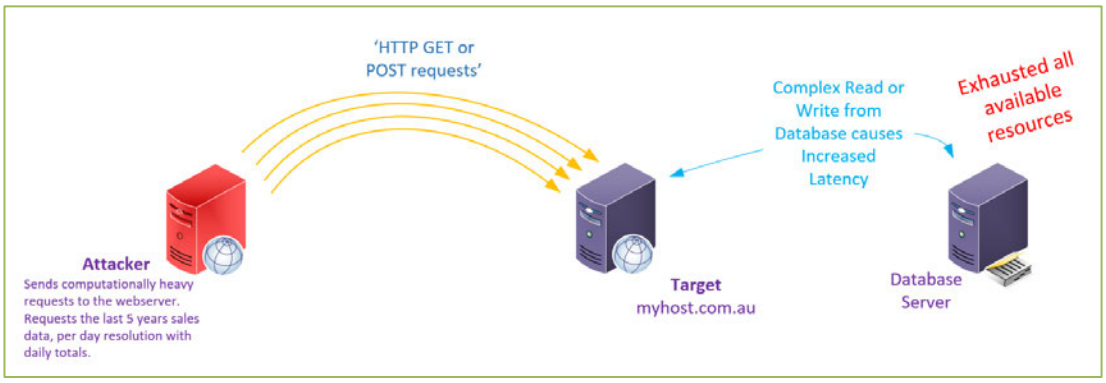


Figure 2.23. Heavy URL (by researcher)

2.10.5 Comparison of Attack Forms

Table 2.3 compares how these attacks are undertaken, some of which, such as volumetric, require very little expertise to achieve. Volumetric attacks are also often easy to detect, which may be one reason why this type of attack has reduced in frequency. SYN attacks, however, have become more prominent (Gutnikov, Kupreev, & Shmelev, 2021).

Table 2.3

Comparison of Attack Forms

Attack form	Type	Aim	Sophistication
UDP flood	Volumetric	These aggressive attacks all aim to consume resources by sending multiple bogus requests.	These are the simplest attack methods. A large volume of requests is required to facilitate this
ICMP flood	Volumetric		

Attack form	Type	Aim	Sophistication
DNS flood	Volumetric		type of easily detected attack.
NTP amplification	Amplified Volumetric	These aggressive attacks all aim to consume resources by forcing the retrieval of larger blocks of data.	These attacks take the principles of DNS, UDP and ICMP flood, but request large replies compared to their request size, making the attack much more efficient
Reflective DNS	Amplified Volumetric		
Smurf attack	Amplified Volumetric	This attack uses IP spoofing to redirect legitimate responses to the target (who never requested them).	Some expertise is needed to modify the packet and spoof the address of the target.
Ping of death (PoD)	Protocol	These attacks interfere with the expected process of the system either causing a buffer overflow (PoD) or a failure to complete handshake process (SYN & SL).	
SYN flood	Protocol		
Slowloris (SL)	Application		Expertise is needed to modify the packets size and spoof the address of the target.
TCP middlebox reflection	Protocol	These attacks use non-TCP compliant middleboxes that amplify small TCP requests into a heavy load for the victim.	
HTTP flood	Application	These attacks aim to tie up system backends with computationally heavy requests.	Expertise and reconnaissance are required to understand which requests create the greatest load.
HTTP flood (cache bypass)	Application		
Heavy URL	Application		

SYN flood attacks can be achieved by the attacker configuring their source firewall to drop any incoming SYN-ACK responses, but this does expose the attacker's IP address, which once detected can be blocked by the target. However, if the attacker is using a very large botnet, there may be thousands of IP addresses to block, which would be time consuming for manual intervention but a smaller task for automation. Alternatively, the attacker could alter the source IP in the packet header, which would prevent the SYN-ACK being responded to and hide the attacker's real IP address.

Therefore, SYN flood attacks have become a fairly simple but effective method of attack, even if they are easily detected.

Application attacks are more complex and require an understanding of the target system, as they are aimed at exploiting requests that place heavy loads. They do not require spoofed IP addresses and use the same paths that legitimate traffic takes. Therefore, they pass undetected through deliberately open firewall ports, and when low rates of request are used, they also fail to trigger bandwidth usage alerts (Nyman, 2018). Deeper packet and traffic analysis is required to detect and then mitigate these types of attack.

2.11 DDoS Trends

The trend has been for DDoS attacks to move from small, extortion-driven groups to politically motivated occurrences and larger groups that use increased complexity and sophistication (Mansfield-Devine, 2015; Nazario, 2008). Complexity and sophistication require further discussion, as examples of the outcomes are not restricted to the immediately observed negative effects of the disruption. Observed secondary outcomes such as malware inserted during the attack and financial/personal data being stolen during the attack highlight that DDoS attacks are beginning to be used as a cover for other nefarious activities (Pitlik, 2019; Wueest, 2014).

For a DDoS, volume does not seem to be important. Research company Neustar observed that 40% of attacks (in its study period) were less than 5 Gbps, but just over a third (36%) of responders had found malware installed during the event. The fact that nearly half of the financial sector responders (43%) also found malware suggests that, in many cases, the DDoS attack was used as a delivery mechanism with the true target being theft (Shah, 2012). However, diversion tactics have not been limited to banking targets. Geopolitically motivated activism (hacktivism) has also used this distraction method to steal valuable information, and they have also used DDoS directly to satisfy grudges where differences of opinion exist.

Overall, as shown in Figure 2.24, several motivators for DDoS use have been noted (Anstee et al., 2017; Bienkowski, 2016).

- Vandalism – Small groups trying new ideas to gain notoriety or for pure

discovery.

- State/activism – Retaliation against politically based decisions.
- Grudge – Similar to state/activism but on a smaller, more personal scale.
- Extortion – Organised crime seeking to profit from hostage/ransom techniques.
- Distraction – Organised criminals or activists seeking to pilfer currency and/or information.

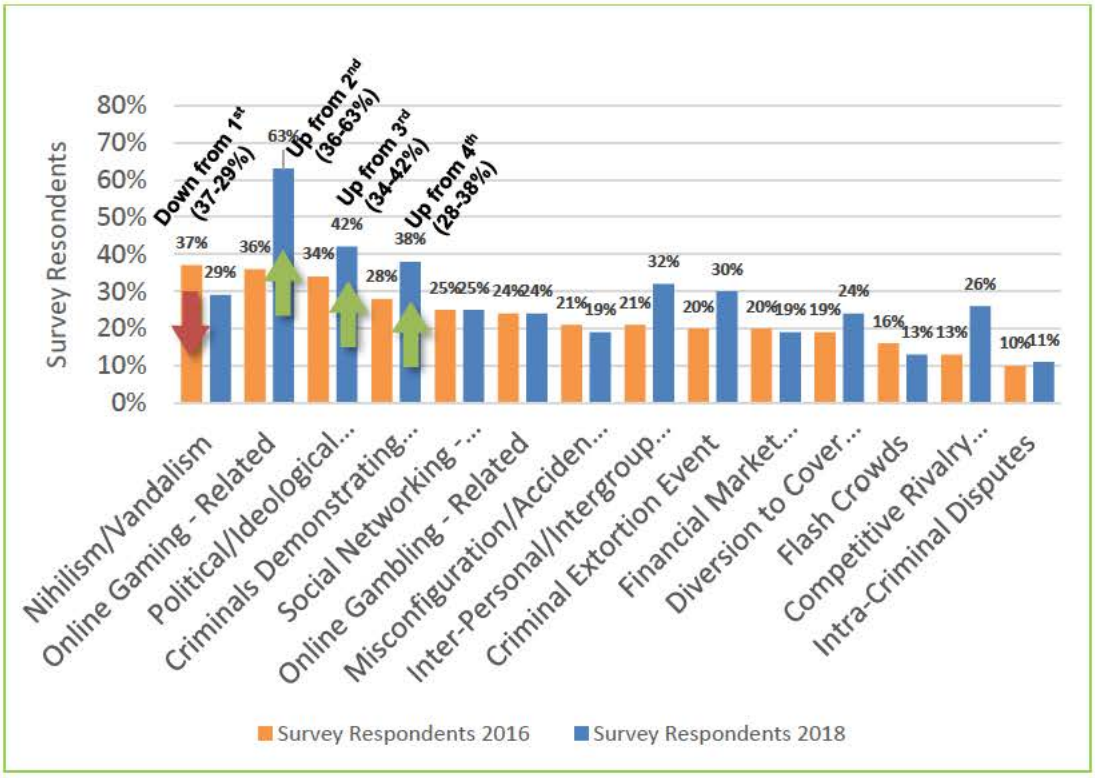


Figure 2.24. Top DDoS motivators 2016–2018 (adapted from Bienkowski (2016) & Netscout (2018))

In these classifications, generally, the larger more prolific cases were performed by organised teams. For example, in 2016, US company DYN was the victim of an attack by 100,000 dispersed endpoints for an entire day (Woolf, 2016) with a magnitude of around 1 Tbps. This is in contrast to the 2010 100 Gbps maximum volume. Attacks of these volumes are likely to increase due to the availability of insecure internet devices, as was highlighted by a 2016 report detailing the use of millions of internet-connected cameras in the disruption of the security news site *KrebsOnSecurity* (Franceschi-Bicchierai, 2016; Goodin, 2016). Concern for types of threat have also changed over time. Malware and phishing were of most concern in 2017, but in recent years large increases in concern have been seen for both ransomware and DDoS (Figure 2.25).

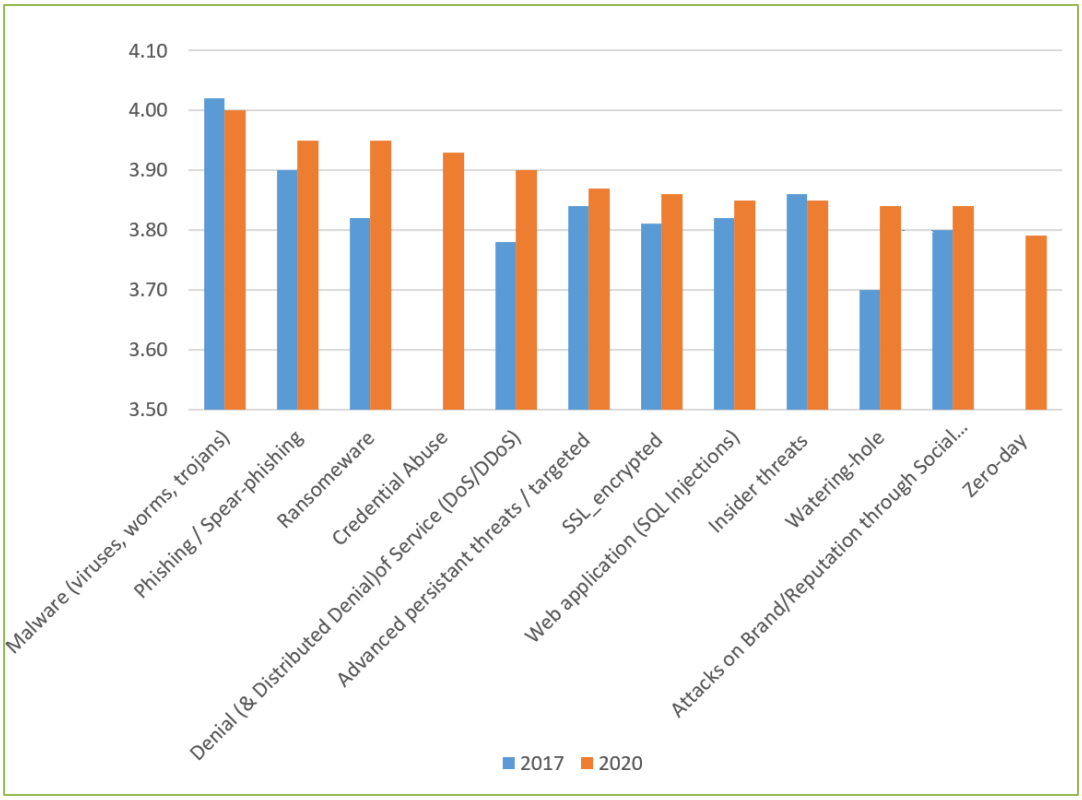


Figure 2.25. Cyber-threat concern 2017–2020 (adapted from CyberEdge Group (2017, 2020))

Ransomware in 2020 occupied the third most concerning threat, up from fifth in 2017, and DDoS rose to fifth in 2020 from its ninth place in 2017 (CyberEdge Group, 2017, 2020). More concern was indicated for account compromise and misuse events, but concern over insider threats decreased. This coincides with increased migration to cloud environments, so this result could reflect the greater governance surrounding cloud domains but may also be due to a reduced innate visibility of remote and indirectly accessed infrastructure.

In 2020, a CyberEdge report showed that 80.7% of organisations in the USA had suffered a successful cyber-attack during the previous three years, which was an increase of 2.7% over the figure reported for 2019 (CyberEdge Group, 2020). Of these, 35% reported they had suffered six or more successful attacks in the same period (CyberEdge Group, 2020). A Verizon report showed that in 2020, nearly 80% of externally coordinated cyber breaches were associated with organised crime (Verizon, 2021), which is far higher than the 30–40% attributed to criminals in 2018 (Netscout, 2018). The increase in organised crime-led attacks and the increased prevalence of DDoS as an attack method are statistics that should be monitored over the next few

years. The likelihood of attack and the increase in volume, sophistication and frequency could be fuelled by the increasingly available IoT devices being integrated into the internet network, but it could also be increased criminal activity that is making the growth more visible.

A report by Verizon acknowledged that DDoS cyber events were common but added that due to the underlying mechanisms that make up the internet, extremely large DDoS are still a rare event (Verizon, 2021). Mitigation methods in 2021 could be provided at multiple points such as ISPs and CDNs, and if each played its part in mitigation, smaller attacks could more easily be accommodated (Verizon, 2021). That said, attacks are still increasing in both frequency and sophistication; therefore, recommendations to be proactive and plan a response have been clear (Mansfield-Devine, 2015; Nazario, 2008).

2.12 Detection and Mitigation Methods

When considering methods of detection and mitigation from DDoS, it helps to be reminded of the three elements required to perform a successful attack.

1. An attack source infrastructure such as the botnet.
2. A target, which is the one who is chosen to be attacked.
3. Attacker motivation, which is instilled in the person who is driven to perform the attack.

The removal of any one of these elements removes the possibility of attack.

As stated in Point 1, DDoS attacks need access to a supply of distributed, controllable systems with which to generate the targeted requests or data streams necessary to provoke the desired response. Historically, these generating sources have come from the many systems that attackers have previously infected with control code, which have been distributed through viruses and malware via transport methods such as websites and email. Therefore, one method of prevention may be to prevent the infection of systems, which would reduce the availability of controllable nodes. However, while antivirus and malware protection are reasonably effective, they play catch-up to the virus and malware creators (Rao et al., 2014). Also, with the introduction of various forms of internet-connected devices (security cameras, coffee machines) that by design have little or no security considerations (Palmer, 2020), the

number of potential compromisable targets has increased exponentially. As a result, DDoS events are now able to combine distributed bandwidth with complexity, and with organised crime commercialising this disruption technique, the explosion in the number of connected devices (quaintly referred to as “the Internet of Things (IoT)”) will likely drive an increase in the occurrence of DDoS events.

DDoS attacks essentially work when an attacker ties up all available resources on a target system, thereby leaving no resources available to be used by legitimate users. A large or unexpected increase in network traffic, as in the case of a volumetric DDoS attack, would be relatively easy to detect, and if an attacker is from a single source, removing the source (Point 1) becomes a relatively simple network configuration that ignores all traffic from that IP address or blackholes the traffic and routes it to a non-existent host. However, while a volumetric attack may be easy to spot, mitigation becomes more difficult. Distributed attackers may be located throughout the world, so removal of the source or manual blackholing of a single or a range of IP addresses becomes complex and time consuming. Increasing the range of blocked IP addresses may be a simple fix, but this comes at the cost of losing traffic from legitimate sources. Similarly, automating the response may allow more rapid mitigation and may allow the system to capture a wider array of attack sources but legitimate traffic may still be lost due the accuracy involved with determining which traffic is legitimate and which is not.

A sophisticated attack can be much more difficult to detect. Sophisticated DDoS attacks that seek to consume system resources, such as heavy URL or SYN flood, could easily be lost amongst legitimate traffic, and detection may require increased analytics and packet inspection. It is possible to inspect each packet to determine legitimacy, but this would come at a cost to network efficiency, increased system load and ultimately an increase in latency. Therefore, effective DDoS mitigation relies on careful planning and thoughtful investment in service providers or often costly technology.

There are multiple strategies from which to approach the DDoS problem, including reducing the potential target, transferring the management or simply accepting that an attack will happen and plan for the consequences. Small businesses or organisations that do not manage their own infrastructure may transfer the responsibility to their

ISPs and cloud operators by procuring DDoS prevention services as add-ons to their existing contracts, but for those managing their own in-house infrastructure, simple and low-cost options for mitigation start with configuring systems to only expose the necessary points of access and configure these to only accept expected request types. For example, preventing direct access to SQL backend servers and dropping unexpected ICMP requests at the firewall can help to narrow the potential targets available and the potential methods of attack.

Larger organisations that may operate using hybrid cloud models and more complex infrastructure may seek to implement detection and mitigation methods that are focused more directly on DDoS. Detection methods may include intrusion detection systems (IDS), which are able to read logs from connected systems (firewalls, routers, servers) and compare the content against stored signature behaviour patterns in order to generate an alert (Jing & Wang, 2020). However, while this method works well for known events, it lacks the capability to detect newly evolved attack methods. In contrast, anomaly detection compares traffic characteristics against established 'normal' operational parameters so that excess volume or excess requests of a particular type can trigger an alert. There is no need to store a library of known attack patterns with this method and therefore it is a flexible approach. However, this method may suffer from false positives as it may not cater for legitimate excess load. As such, anomaly detection methods that utilise machine learning (ML) and AI are under development (Bdair Alghuraibawi et al., 2021) to help increase the efficiency and accuracy of this method.

At this level, mitigation methods that inspect each packet to determine its legitimacy can be performed so that valid traffic can be allowed through to the destination and bogus requests dropped. Automation, ML and AI can all help to reduce the latency that packet inspection creates, but this method will continue to incur a performance cost (Fortinet, 2017). If in place, software defined networking (SDN) can be used to automatically adjust network traffic paths and route suspect traffic to "scrubbing services" (Salopek et al., 2022), whilst traffic with higher confidence of legitimacy can continue to use normalised paths. In addition, further methods to improve DDoS detection and mitigation are continually being researched (Ramprasath & Seethalakshmi, 2021).

2.13 Information Sharing

Since the early days of ‘phone phreakers’ using bulletin boards (BBS) to collaborate (Kizza, 2017, p. 111), hacking groups have found ways to share information. The modern-day equivalent of the old BBS can be found on the dark web (Palmer, 2016), which is a hidden collection of internet sites and forums that can only be accessed using a specialised anonymisation TOR (The Onion Project) web browser. Access to these forums often require sufficient reputation or invitation (Palmer, 2016), but once approved, hackers are able to access hacking tools for use or to further develop and add to the hacker community’s capability.

It therefore follows that organisations that actively share knowledge and threat intelligence information aid the improvement of defence strategies, including prevention and mitigation and whether these attacks are generated by an individual or group, either locally or from other countries. Growth in threat intelligence is fuelled by cybersecurity professionals’ ability to share their experiences of incidents and their own threat information. In their study, Ahmed and Roussev (2018) found that peer instruction in cybersecurity was very useful, and also recommend this approach to other subjects. However, the cybersecurity teams in businesses and organisations do not seem to operate in the same way. Managers undervalue information-sharing in cybersecurity specialists’ professional development (Brilingaitė et al., 2022), and this lack of sharing may be due to perceived technological, legal and psychological obstacles (Brilingaitė, Bukauskas, & Juozapa, 2022). This position contradicts much of the research in this area.

Sedenberg and Mulligan (2016) suggest that rational sharing of best practices, threats, risks and vulnerabilities provides an advantage to the group and that this collaborative stance should be adopted. However, there are barriers to this sharing, such as the complexity of the topic, which is made more difficult due to the lack of a common language, and if the barriers appear greater than the incentives, sharing is unlikely to occur (Koepke, 2017). The lack of a common language becomes more apparent when collaborating with other countries. As cyber-attacks are commonly delivered across international borders, limiting knowledge transfer between local organisations is not effective, and inter-country collaborative efforts should be adopted (Bourgue et al., 2013; ENISA, 2016).

The potential for negative consequences, such as reputational damage following the accidental release of private infrastructure information, is another reason for reluctance to share information (Nweke & Wolthusen, 2020). Cybersecurity information often contains sensitive information and private data, so Wagner et al. (2018) suggest a trust taxonomy in order to share sensitive data within the cyber defence community.

2.14 Summary

This chapter explored a wide range of practitioner-based literature surrounding cybersecurity. It began by looking at the growth of technology, including the arrival of the internet and the parallel emergence of hacking groups that aimed to interfere with the technology available at the time. The literature showed that, after some time, organised criminals and activists found new uses for the capabilities developed by technology enthusiasts, and this along with the introduction of large numbers of IoT devices has resulted in the severity of DDoS growing from a cybersecurity annoyance to an attack that could result in measurable reputational damage and loss of productivity.

As well as the historical record, this chapter covered how some of the more common forms of DDoS attack are undertaken. Their aims, ease of detection and level of expertise required to accomplish them were explained. Discussion of the approaches to detection and mitigation showed that this is an area of industry focus and one that industry is continually working on to counteract these disruptive attacks. The practitioner literature appears to be heavily focused on technological solutions, with little information regarding the human side of the defence capabilities. This and more are discussed from an academic perspective in the next chapter.

Chapter 3: Literature Review – Academic

3.1 Introduction

This chapter reviews the literature sourced from academic scholars and researchers, beginning with an overview of the important factors and events that led to the creation of the modern-day internet. The internet began as a result of military effort (Adams & Scolland, 2006), and the review acknowledges the role of cyber in defensive and offensive strategies and conventional warfare (Lonsdale, 2004). The ability of cyber-attacks to transcend from the virtual to the physical world is then discussed, followed by a review of the motivation and perspectives of nations, organisations and individuals. Finally, the impacts of the COVID-19 pandemic are raised, as the pandemic has had far-reaching effects on all factors concerning cybersecurity, including people, process and technology.

3.2 Gaps between Practitioner and Academic Literature

Gaps exist between practitioner (industry) literature and academic literature. These gaps occur for several reasons:

1. The incentives to write varies - Practitioner articles are written with the aim of achieving an understanding in order to enable an outcome, whereas the academic literature is aimed at expanding knowledge itself (breadth and depth) through the publication of scholarly articles (Bartunek & Rynes, 2014).

2. A preference for rigour or relevance (Bartunek & Rynes, 2014) - Academics argue that practitioners chase only the evidence that leads to a successful solution, whereas academics prefer methodological, rigorous research that identifies facts even if that knowledge proves to be uncomfortable or challenging (Simon, 2004).

3. Research duration - Academic research tends to focus on longer-term studies that are aimed at future prevention or enablement (Anandarajan & Lippert, 2006). On the other hand, practitioners tend to be more immediately focused and pursue the most

efficient path to completion. Practitioners often do not have the resources to pursue knowledge outside of their directive.

4. Perspective - Those who contribute to industry literature often assume their desired outcome is some form of defence; therefore, their information is written to help the reader understand it from that perspective. Academics aim to provide a complete and defendable pool of knowledge that is available for all, irrespective of the intended use.

Therefore, compared to practitioner literature, academic literature may hold diverse knowledge regarding the researched subject that would help to gain a complete view of the existing knowledge. Thus, it is important to review academic literature alongside practitioner literature in order to gain a more complete view of current understanding.

3.3 Birth of the Internet

As one of the many articles that discuss the founding of the internet, Herpig's (2014) discussion of the early days states that the cold war between the USA and the Soviet Union (in the 1950s) was a significant driver of the project. The ability for the US to perform a "second strike" in response to an attack was widely recognised as a formidable deterrent (Bondarenko, 2018). Prior to the internet, military communications were delivered by nodes that offered single points of failure, and in the event of their destruction, the ability to perform a second strike would be lost, thus neutralising any potential deterrent. The potential of nuclear war therefore drove an awareness of the need for a communication network that would be capable of surviving a nuclear attack, as the US military recognised that precarious communication was a serious vulnerability in their defence strategy (Herpig, 2015).

In the 1960s and 1970s, while working on an innovative packing switching technology, British National Physics Laboratories (NPL) and the American Research and Development Corporation (RAND) worked to create a network that could continue operation even if node failure occurred (Leiner et al., 1997). Initially set up in the University of California, Los Angeles (UCLA), the network, known as ARPANET, utilised the National Control Protocol (NCP), but by 1983 the

Transmission Control Protocol (TCP) (of 1975) had improved to become the Transmission Control Protocol/Internet Protocol (TCP/IP), which is still in use today (Adams & Scolland, 2006; Leiner et al., 1997). However, its early role was to help the exchange of ideas and theory in UCLA, which resulted in the military leaving the project and developing the military network (MILNET) (Adams & Scolland, 2006), which by January 1990 had more than 168 packet switching nodes (PSNs) in the US and a further 57 PSNs throughout Europe and the Pacific (LaQuey, 1990).

For the modern day, these developments had far-reaching effects. By creating a network of networks (Figure 3.1), where local area networks (LANs) connected local devices such as printers, cameras and laptops inside of a physical or virtual boundary and wider connectivity was handled by ISPs that passed the traffic to the rest of the world via an internet backbone, (known as a wide area network (WAN)), network paths between LANs could be fault tolerant and survive node failure by employing routing protocols to transport data along an alternate path. Routing protocols were able to make use of detection capabilities and algorithms that allowed the best alternate route to be selected (based on link state, transport time or an assigned 'cost').

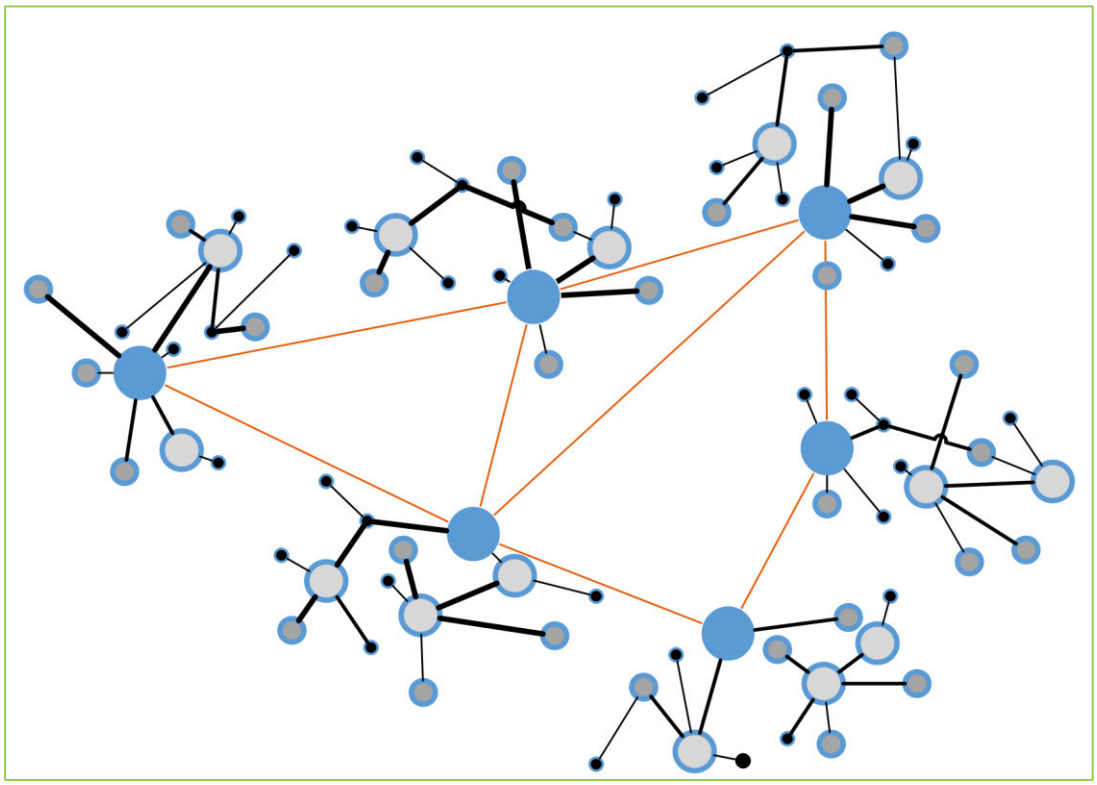


Figure 3.1. Network of networks (by researcher)

This adaptability reduced the consequence of using subsea fibre optic cables to provide inter-country communications. In the event of a subsea cable impasse, whether through equipment fault, accidental damage from ships dragging anchors or deliberate interference from offensive adversaries, network traffic can continue to its destination via an alternate route, even if the alternate route is potentially longer as shown in Figure 3.2.

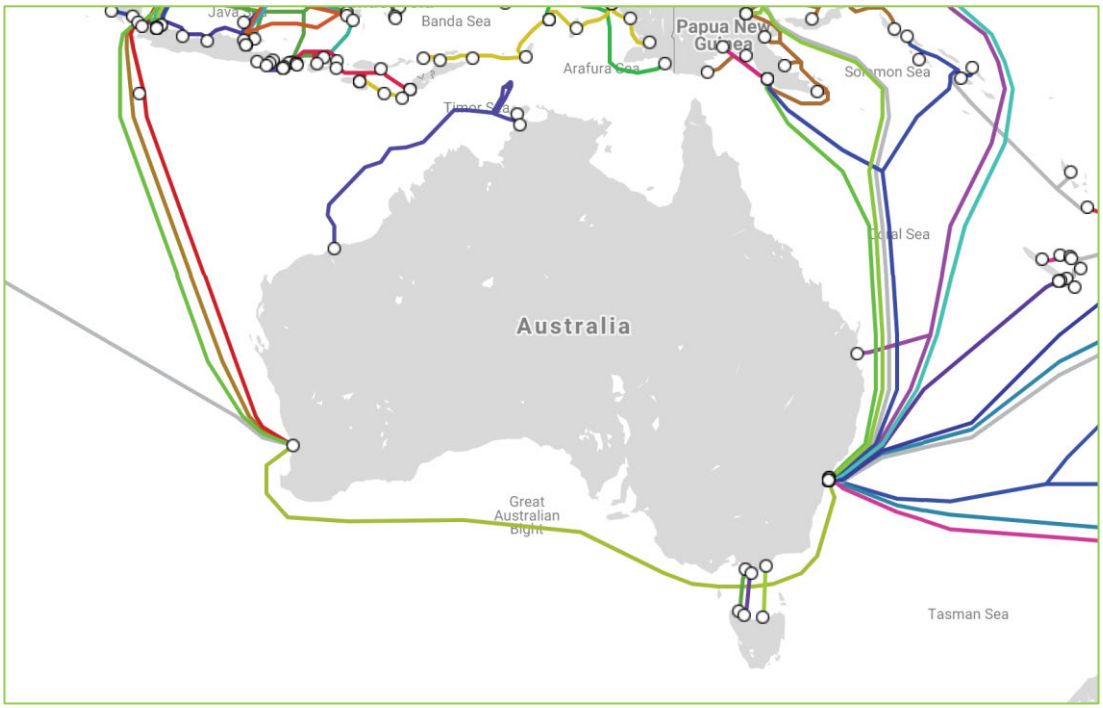


Figure 3.2. Subsea cables connecting Australia (from TeleGeography (2020))

3.4 Comparison of Cyber in Operations to Conventional War

While there are few reports of cable sabotage, with Egypt's loss of two undersea cables on January 30, 2008 being one suspected occurrence (Arthur, 2013; "Of Cables and Conspiracies", 2008), there are many reports of cyber-attacks being used as a weapon of war. While the internet itself has not become a motivator for cyber-attacks, it has become a tool that can be exploited by rival adversaries (Mauslein, 2014), and its role in conflict is now beginning to be understood.

Mauslein (2014) discussed the similarity of cybersecurity events to those of physical war, with the aim of describing the motivations behind cyber-attacks. This view may

be valid, as cyber-attacks had already been seen to have a recordable impact during conflict. For example, in September 2007, the Israeli Airforce acquired control of Syria's air defence systems just prior to Israel's military bombers targeting and destroying a Syrian nuclear installation without detection (Holmes, 2018). In this case, the target was unaware of the cyber-operation prior to the physical attack, so they had little time to react to their loss of defence and no time to negotiate an alternate outcome. In other cases, cyber-operations have been extremely visible and, according to Mauselin (2014), the introduction of cyber-operations may reduce the likelihood of conventional war, as there is a further step in the escalation sequence where diplomacy could be pursued. However, this extra step may have come at the cost of an increase in lower-level hostilities.

The term cyber-operations covers three forms:

1. Cyber-attacks – These are aimed at harming an opponent, whether it is destruction of data, damage to data integrity (Mauslein, 2014) or crippling of infrastructure (Cohen, 2018).
2. Cyber-espionage – This is aimed at the acquisition of intellectual property owned by another entity (Mauslein, 2014).
3. Cyber-terrorism – This includes hacktivism, the aim of which is to convince the target to comply with the attackers' demands (Mauslein, 2014). With this type, there is often little permanent data damage and attackers have been known to help restore services once the target has fulfilled the requests.

The older term "cyber-warfare" is potentially inaccurate, as attacks have most commonly occurred at times when war had not been declared (Herpig, 2015; Mauslein, 2014).

The term "cyber-threat" does not appear in the list as a cyber-threat is simply a threat that only becomes a cyber-operation once it has been actualised. Snowdon (2015) considers all cyber-attacks to be cyber-terrorism, but acknowledges Ahmad's (2012) claim that individuals' perceptions of what constitutes a cyber-threat can differ, as there are many forms to consider:

- Data and service-related attacks:
    - theft and access of personal/private information (PPI) or personally

identifiable information (PII) (Ahmad, 2012)
    - identity theft (Ahmad, 2012)
    - website duplication to obtain identities or payment card information (PCI)
    - interference with financial institutions and their transactions (Ahmad, 2012)
    - Website vandalism (Ahmad, 2012).
- Attacks on physical infrastructure:
    - attacks on oil and gas refineries (Beato et al., 2021)
    - attacks on pipeline infrastructure (Metcalf, 2020)
    - attacks on radar infrastructure (Hounshell, 2007)
    - attacks on nuclear research facilities (Lindsay, 2013).

Any of the three classes of cyber-operations may be used by countries as their conflicts escalate toward a physically destructive war. Also, like other forms of attack, opponents may engage in an oscillatory retaliation as tensions rise. However, as attacks can be easily initiated, countries cannot respond to all aggressive actions (a daily occurrence) and each country will have its own level of irritation that it will tolerate, beyond which war may well eventuate, similar to their physical attack equivalents such as vandalism and propaganda (Herpig, 2015; Mauslein, 2014).

Cyber-operations may be able to encourage the settlement of a dispute but within war, they generally do not wield enough power to be used in isolation (particularly when compared to the devastation caused by explosives) and could not win a war outright (Herpig, 2015). Instead, cyber-operations would most likely be used as a supplemental step, such as an attempt to adjust the balance of power (Lonsdale, 2004). Preceding conventional war with the use of cyber-initiated system disruption or intelligence gathering may create a more significant outcome (Lonsdale, 2004).

Libicki (2007) proposes that cyber-operations can perform three roles during conflict:

1. The capability of adversaries could be crippled if they are caught by a surprise attack.
2. A targeted attack could provide a decisive military advantage.
3. An adversary could be caused to lose confidence in their own systems.

However, in any case, to provide an opportunity for the next step in defence or in an offensive manoeuvre any delivered cyber-attack should be strategically placed (Libicki, 2007).

Information superiority is a key element of success, and conflicts are often born from fear or threat of these differences or the perceived threat from competition (Herpig, 2015). Therefore, the attainment of superior information is a key element for success. This information superiority can be achieved by undertaking cyber-operations against rivals (Herpig, 2015). In order to build sufficient defences, countries should seek to understand the methods of attack used by their rivals and the methods used by any proxied group that the rival may have the ability to influence (Cohen, 2018). Proxies are often used to avoid direct conflict (Cohen, 2018), so while advanced countries are able tolerate low levels of cyber interference, their defences should be constructed to defend against more sophisticated attacks (Cohen, 2018).

3.5 Rise of Cyber-Operations

As the internet grew and expanded its coverage, so too did the magnitude of discussions surround cyber-operations. In addition to the fictional 1983 movie *War Games*, Herpig (2015) highlights that Clifford Stoll's (1989) book, *The Cuckoo's Egg*, details his search for a computer hacker who gained entry to military sites via the Lawrence Berkeley National Laboratory. However, the first academic discussion took place in 1993, when John Arquilla and David Ronfeldt discussed the value of information and how the Mongol war strategy reflected those strategies that may be employed during future cyber-warfare (Arquilla & Ronfeldt, 1997).

These historical texts acknowledge that some understanding of cyber-operations has been present since the late 1980s, but Herpig (2015) highlights two schools of thought. The conventional school, which is supported by Schneier (2009), Libiki (2009), Arquila and Ronfeldt (1997) and Rid (2013), believes that cyber-operations are merely tools that can be used to supplement traditional or conventional war, as alone they currently lack the power to create a significant outcome (Herpig, 2015). For example, a cyber-equivalent of a Pearl Harbor outcome is deemed by the conventional school to be overrated and unlikely (Schneier, 2009). By contrast, the unconventional school, which is supported by authors Clarke and Knake (2010), Chase Cunningham (2020)

and Janczewski and Colarik (2008), believe that cyber-operations are dangerous and a serious threat to a nation's security, as many nations have critical infrastructure connected to the internet, thus making them a potential target. The Stuxnet attack on Iran (Farwell, 2011) is a good example that supports the unconventional school's belief that the aforementioned cyber Pearl Harbor is just an event waiting to occur.

Both schools of thought acknowledge that cyber-attacks will eventually become severe, but the debate is around the view of the current level of risk imposed by cyber-threats, as the unconventional school believes that the time has already arrived (Herpig, 2015).

3.6 Ability to Break Out of the Virtual World

Prior to the Stuxnet attack on Iran in 2010, there had already been several high-profile attacks.

- In 1999, Chinese hackers used a DDoS to interrupt the US Government's website www.whitehouse.gov for three days (Hunker, 2010; Messmer, 1999).
- In 2000, several large corporations, CNN, Dell, E-Trade, eBay and Yahoo, were the target of an attack by a 15-year-old child, Michael Calce (Cloudflare, 2019).
- In 2007, Estonia suffered three weeks of DDoS attacks against government, commercial and financial institutions (Grimes, 2007; McGuinness, 2017).

The Stuxnet attack presented a change of outcome. Rather than hijacking, destroying or stealing information, Stuxnet used compromised computers to physically destroy centrifuge equipment. Stuxnet spread indiscriminately via Microsoft Windows but was highly targeted, and its aim was to only disrupt the Supervisory Control and Data Acquisition (SCADA) systems it could identify (Fruhlinger, 2017). SCADA systems were used in Iran's nuclear program to control centrifuge equipment. Stuxnet instructed the centrifuge to spin at a much higher speed than was specified, which caused damage or destroyed the equipment, while at the same time reporting back that all was within tolerance limits (Fruhlinger, 2017).

Brenner (2009) further highlights that new cyber-attacks are aimed at transferring the disruption and damage to digital information into the physical world. Israel's disruption of Syria's air defences led directly to the physical destruction of Syria's

nuclear development sites; however, Brenner also mentions the potential for cyber-attacks to disrupt hospital information, which would result in the potential for patient harm. Sadly, in September 2020, this potential was realised. A group of attackers targeted the systems of a German university but a mistake by the attackers misdirected their attack, which resulted in an attack on the Dusseldorf University Hospital instead. This disruption led to the death of person who failed to receive the immediate and acute care they required (Tidy, 2020).

3.7 Motivations for Attack

As previously mentioned, for a DDoS attack to occur, there are three distinct requirements:

1. Infrastructure, including the source pool of controllable devices (e.g., the botnet), the network capable of delivering the attack and the connected endpoint devices that will be attacked.
2. Target, which could be an individual, entity, organisation, cause or other point of focus.
3. Motivation that is strong enough for an individual or group to move from idea to action.

Removal of any of these three factors would leave a state where DDoS cannot occur. Infrastructure is well known and well reported as it undergoes continuous improvement when owner-operators seek to increase the resilience and security of critical services. Targets and motivation are equally as important for DDoS; however, in contrast to infrastructure, targets and motivation are less visible.

3.8 Perspectives

Targeted or accidental victims have not always publicised the occurrence of these hostile events, and the motivation of the attackers can also be obscured. Even when the attackers are uncovered, the motivation for the attack may sit with another unidentified group that may have procured the services of those more technically minded. In the case of the Dusseldorf University Hospital attack, the perpetrators were not motivated to cause human harm but instead were motivated to cause chaos so that their target would be encouraged to meet the perpetrators' financial demands (Tidy,

2020). In the case of the 2013 DDoS attack on Spamhaus by a group called Stophaus, the motivation was revenge (Jenkins, 2014), whereas the Estonian Government DDoS of 2006 was a politically motivated attack. In each case, it has taken some time to uncover the motivation behind the attack.

There is currently little understanding of target selection and corresponding motivation for attacks; therefore, in order to understand this more deeply, information can be reviewed from three perspectives: the individual perspective, the organisation's perspective and the country perspective.

3.8.1 Individual Perspective

The human factor often facilitates a weak link in cybersecurity (Wiederhold, 2014). For example, if an individual generally has a low risk assessment of the need to protect their own identity online and invokes a correspondingly minimal approach to their protection, this behaviour may carry over to workplace computers, exposing organisations to cyber-threats (Huang et al., 2010).

Individuals have differing needs, and several theories exist that attempt to understand the way individuals are motivated to perform actions and decisions. Two of these, McClelland's (2010) "trio of needs" and Maslow's "hierarchy of needs" (as cited in Tanner & Raymond, 2012), approach this understanding from different perspectives. McClelland's (2010) theory aims to understand an individual's internal desires by classifying their primary drivers as either achievement, affiliation or power, whereas Maslow's theory aims to show the order in which needs must be met to reach an individual's preferred level of satisfaction (Tanner & Raymond, 2012).

In McClelland's (2010) theory, each of the drivers focus on the outcomes of the individual rather than their group. Even in the case of the affiliation driver, the aim of the individual is to feel comfort through group acceptance, whether or not the group seeks to provide the best outcome for the organisation. From Maslow's point of view, irrespective of the internal desires of the individual, they are driven to address basic needs before they can contemplate needs of a higher form. According to Maslow, safety would need to be sought before power could be considered, but again these drivers are from the perspective of the individual, not the group or what the group

needs (Tanner & Raymond, 2012). These two theories share a commonality of agency theory, which states that along with being risk adverse, humans are egoist and possess bounded rationality (Bosse & Phillips, 2016). Under agency theory, organisations assume efficiency is the success criteria, but also that there is an imbalance of knowledge between parties and potentially conflicting goals (Bosse & Phillips, 2016). This lack of cohesion or alignment between government or organisational groups and individuals exposes weaknesses in what may otherwise be well-intended defence strategies.

Technology alone cannot address the perception of cyber-threats. Involvement on three fronts (people, process and technology) must be addressed to gain effective information security (Herath & Rao, 2009). The human factor remains the weakest link in cybersecurity (Kolenko, 2019; Wiederhold, 2014) and, therefore, human behaviour has a significant effect on vulnerabilities (Kolenko, 2019; Wiederhold, 2014). Enabling people and training them in the use of theoretical frameworks (statistical, probabilistic, methodological) can affect reasoning and behaviour (Nisbett et al., 2001), thus potentially reducing risk, but as psychological processes are susceptible to community and cultural influence, thought processes between groups may vary. This provides an advantage, as increasing diversity in organisations may bring a breadth of knowledge and new understanding, but culturally influenced desires may establish goal conflicts, such as quality of the solution versus speed of delivery, even when a common organisational goal is agreed. Snowdon (2015) believes that individuals should understand that while all share a concern for cyber-threats, their individual perceptions may be different, and once the existence of a difference is acknowledged, individuals can reflect on their own attitudes, then consider if their behaviour requires modification/refinement in order to become more safety-conscious in the online environment. Agency theory's egoist assumption would align with this view; if online safety is a personal concern, an individual may be more likely to modify their behaviour to the benefit of the organisation.

Protection motivation theory (PMT) (Rogers, 1983) is a theory that proposes individuals protect themselves based on six factors (Ifinedo, 2012):

1. perceived **severity** of a threatening event
2. perceived probability of the occurrence or **vulnerability**

3. efficacy of the recommended preventive behaviour (the strength of the preventative plan)
4. perceived self-efficacy (the confidence one has in one's own capability to invoke the defensive plan)
5. level of protection motivation
6. protective behaviour

Considering two elements of PMT, severity and vulnerability, a possible relationship between PMT and an employee's perception of cyber-threats could be understood (Snowdon, 2015). This is apparent as the employee's perception is built on several reflections.

1. The employee may proactively choose to implement organisational security practices or may be resistant to change even when the organisation considers the changes to be in their best interest (Snowdon, 2015).
2. The employee may or may not consider themselves to have an active responsibility for keeping access to systems and data in their control secure and, therefore, may invite or resist technology changes when they seek to improve the level of cybersecurity in place (Snowdon, 2015).
3. How the employee considers compliance with protocols and their awareness of any access or interception of data that falls outside of expected and authorised behaviours (Snowdon, 2015).

With cyber-attacks, many of the sensory indicators are hidden, as cyber-attacks, being digitally based, often do not provide sufficient information, unlike threats that occur in the real world (Wiederhold, 2014).

Enabling individuals and training them can affect their reasoning of events and even their behaviour (Nisbett et al., 2001). Therefore, defining processes and providing training are common methods used to reduce risk and develop evolving operational ways of working. However, Hofstede et al. (2010) believe that individuals learn ways of thinking and potential behaviours through their life, and Schjolberg and Ghernaouti-Helie (2011) outline a growing body of evidence that supports a link between culture and the behaviour of cyber victims and their attackers. Therefore, as community and culture have the ability to influence individuals' patterns of thought, the ultimate thought processes between different groups may vary (Nisbett et al., 2001). As such,

local culture, ethics, law and politics have become connected to online cyber behaviour (Schjolberg & Ghernaouti-Helie, 2011); however, the information industry continues to focus on the technology used in threat protection rather than the culture of the individual or group actors (Hofstede et al., 2010).

In addition, an individual may be driven towards any of the needs defined by McClelland (2010); therefore, despite the agnostic nature of technology, the way a technology is applied by individuals and groups may differ, resulting in diversity of outcomes. Individuals solve problems in different ways. Some of these differences can be influenced by cultural upbringing, and this may affect how cyber-defence operations are conducted and how similar technology can be in place but ultimate vulnerability may be highly variable.

The relationship between social culture and cyber-operations is important as culture is supported by an individual's values, which are acquired through the individual's life experiences (Rokeach, 1973). Although they can be influenced by environmental factors and collective group behaviour, these values tend to be long lasting. Values are learned and adopted by groups and become and remain stable over time; therefore, the culture these values support directly affects how a country behaves (Karahanna et al., 2005; Rokeach, 1973). Uncovering this relationship allows for predictive capabilities for cyber-operational outcomes (attack and defence) to potentially occur, and with this, the possibility to influence or direct cyber-operational actors becomes available.

3.8.2 Organisational Perspective

Snowdon (2015) suggests that the IT industry should respond aggressively to cyber-threats and ensure that their employees are sufficiently educated on the potential and opportunity for cyber-attacks. In addition, as per Foltz (2004), employees should be aware of the various methods in use by cyber-terrorists, as well as their potential targets. Digital disruption has allowed IT systems to reach much deeper into the day-to-day mechanics of 21st century life, bringing ease of living but also much stronger dependency on IT. Along with this improvement of living standards comes a broader field for cyber actors to identify vulnerabilities (Chittester & Haimes, 2004), so it becomes vital that employees are aware of the potential for attack. Employees must fully understand the outcome of their actions and be proactive in the protection of

themselves and the information they are entrusted with. In turn, organisations should stretch their interest from the business to include the employees and how they use computers and the internet in the course of their work (Snowdon, 2015). Organisations should not take employees' attitudes to cybersecurity for granted (Huang et al., 2010) and should implement monitoring and policies that ensure benefit to the organisation. Further, organisations should seek to understand the efforts their employees make to protect their personal data, as Snowdon (2015) found this relationship has a statistically associative connection with an employee's perception of what constitutes a cyber-threat.

Organisations use SWOT analysis to analyse their strengths, weaknesses, opportunities and threats so that they can find ways to improve their weaknesses and build strategies that are aimed at capitalising on the opportunities that their strengths support (Omer, 2018). While a SWOT analysis focuses on internal organisational aspects, organisations use the PESTEL framework to analyse key outside influences. The PESTEL framework examines political, economic, social, technological, environmental and legal influences. When examining environmental effects, this extension of Francis Aguilar's PEST framework (Rastogi & Trivedi, 2016) provides a way of identifying high-level attributes and, with that, begin to form strategies to minimise the impact of threats while supporting the exploitation of opportunities. This high-level approach provides a suitable method for understanding how changing attributes affect a country's security posture.

3.8.3 Country Perspective

Using quantitative methods to examine historic events, Mauslein's (2014) research used aspects that could be classed within PESTEL factors to show how political, social and economic characteristics might influence the likelihood of a state being attacked. The research concluded that several attributes may be indicators of potential victims (Mauslein, 2014).

Robustness of the economy

Economic factors such as a country's Gross Domestic Product (GDP) per capita could be one determining factor. Due to the costs of internet infrastructure development, Xiaoming and Kay (2004) were able to surmise that countries with a high GDP per capita would have deeper internet coverage, and if deeper internet coverage expanded

the attack target area, then the potential for attack may increase. However, Mauslein (2014) found that the sturdiness of a country's economy is an additional attribute that requires consideration. For example, while GDP increases often translate to higher likelihoods of being the target of cyber-terrorism, there may be an exception when the country's economy is robust (e.g., USA) (Mauslein, 2014). Increased GDP per capita creates a country that is viewed as a more attractive target for cyber-espionage, as this increased availability and increased desire by opponents produces an increased likelihood. However, there is a point where the country's expenditure on cyber-defence reduces the attractiveness and the opportunity begins to reverse. Therefore, from a technological perspective, a GDP per capita increase reduces cyber-terrorism, potentially due to increased investment in cyber-defences (Mauslein, 2014).

Regime and freedom of speech

A political factor that potentially influences attack likelihood is the country's regime. Using the Polity IV scale (Marshall et al., 2019), attack frequencies appear to vary depending on whether the regime aligns more with an autocratic or democratic society (Mauslein, 2014). From a social perspective, the relaxed control in democracies allows groups to form in order to permit peaceful conflict resolution. However, while democracy may permit peaceful negotiation, this is not always the outcome. Permitting groups to form also allows terrorist groups more freedom of movement, which increases the opportunity for attacks to occur. From a legal perspective, assurance of citizens' political and civil liberties in a democracy lowers the risk and penalty for committing terrorism, which, in turn, could lead to an increase in terrorist activity (Q. Li & Schaub, 2004).

Social Indicators

Henshel et al. (2010) support the view that cyber-security resources may be used differently by diverse cultures, and this may positively or negatively impact on defensive cybersecurity positions. Examination of the social aspects of a nation-state's culture may provide information on the level of risk imposed and the level of tolerance.

Hofstede et al. (2010) discuss a framework that could be used to assess cross-cultural behaviour patterns. The research highlighted six dimensions:

1. Power distance (PD) – This relates to the power difference between leaders and everyone else. In cultures where it is accepted that leaders are considered

to be better than others, this is classed as a large power difference (LPD). Conversely, small power differences (SPD) are where all are considered equally important and leaders can easily be replaced.

2. Individualism/collectivism (IDV) – This considers whether individuals feel independent or more as part of a group.
3. Femininity/masculinity (MvF) – In a society classed as masculine, the genders are distinguished and winning is celebrated. In a feminine society, the genders are more equal and there is wide-ranging sympathy for the underdog.
4. Uncertainty avoidance (UAI) – This compares cultures that have a preference for continuity against those with a tolerance for uncertainty.
5. Long/short-term orientation (LvS) – Long-term cultures accept that their world continues to evolve and, as such, will continue to plan. Short-term cultures place more focus on reflection and use history to direct how life should be. They believe the world will remain as originally created.
6. Indulgence/restraint (IvR) – Indulged cultures feel free, enjoy friends and believe life is good. Restrained cultures find that life is hard and believe that it is normal to have to perform one's duty.

Kolenko (2019) found there were measurable relationships aligned with several of these dimensions. Victim behaviour tended to be more masculine (Kolenko, 2019) and potentially exhibited a level of overconfidence (Hofstede et al., 2010), which could lead to IT vulnerabilities through exploited blind spots. For more communal systems, such as a network DNS, feminine cultures have performed better. For example, the more nurturing nature of feminine cultures have been found to be more interested in protecting the DNS records of others as well as their own, and this attribute aligns with another Hofstede et al. (2010) dimension of orientation, with short-term oriented cultures less inclined to invoke fuller protection. By contrast, feminine long-term orientated cultures may provide a greater defence.

While examining SQL injection attacks, Kolenko (2014) found that attackers generally came from cultures that prefer stability over change (a high UAI), and their targets were the opposite, being more comfortable with uncertainty. Cultures with a low UAI that prefer "few and general rules and laws" may potentially be deemed a soft target (Hofstede et al., 2010). Similarly, those countries with a high PDI may,

through promoting the strength of their superior leader, present a target that invites opposing cultures to attempt exposure of their vulnerabilities (Kolenko, 2019). This view aligns with that of Sample (2013), who found a statistical relationship between high PDI cultures and vandal/defacing types of attack.

Military size and international conflicts

Statistics show that the size of a country's military has an impact (Mauslein, 2014). Countries with a larger military have higher levels of cyber-threats, cyber-attacks, cyber-terrorism and cyber-espionage (Mauslein, 2014), which means that a country with a large army is much more likely to be a target for cyber-operations than those with smaller forces. Added to this is the discovery that ongoing conflict or war increases the frequency of cyber-terrorism (Mauslein, 2014). Therefore, if a country increases the size of its military capability in response to an ongoing or potential conflict, these two factors may coincide to further increase the likelihood of cyber-operations occurring. Thompson and Dreyer (2012) highlight that while an existing international rivalry serves to increase the probability of warfare, democratic peace (between the same countries) does not wield the same power. That is to say, democratic peace has less ability to decrease the probability of warfare than rivalry has to increase it (Thompson & Dreyer, 2012).

Mauslein's (2014) statistical analysis in part shows evidence that a country's move to rivalry status corresponded with a reduction in cyber-threats. This supports the work of Valeriano and Maness (2014), who believe that as cyber-threats could be perceived as an act of war, countries may refrain from participating from fear of escalation tensions. However, this finding is contrary to that of Findley et al. (2012) and Conrad (2011), as they found that rival countries have used cyber-terrorism instead of a costlier military war, which suggests it is likely that there is a level of cyber-terrorism that may be tolerated before escalation occurs.

In his statistical analysis, Mauslein (2014) also found support for an opposite argument. In some cases, an increase in rivalry corresponded to an increase in cyber-threats. One possible explanation could be the level of information one side has on their rival. If one side has obtained information regarding a rival's level of tolerance for cyber-attacks, they may be more confident to increase their efforts knowing there is little risk of an armed response. This would suggest that peace is preferable to

warfare when levels of aggression remain below an acceptable tolerance. This is evidenced by the Titan Rain attack, which was discovered in 2005 (Council on Foreign Relations, 2005). Over several years, Chinese-located attackers used Titan Rain to steal 10-20 Tb of data from the US (Crowell, 2010) and the UK (Council on Foreign Relations, 2005) that included secrets, military information and technology. While the attack greatly increased the friction between China, the US and the UK, conventional war did not occur.

Qualitative analysis of historical events suggests that when a country has been targeted by cyber-espionage, they are more likely to bargain for peace if the risk of conflict will lead to more than 1,000 casualties, but if the risk of casualties is lower than that limit, countries are more willing to react violently to the exposure of their digital property (Mauslein, 2014).

In recent years, Israel has suffered greatly from cyber-attacks. In response, they have not only built capable defences, but have also marketed themselves as a world leader in that field (Cohen, 2018). The Israeli Government has invested in start-up businesses and the development of cyber tools (Cohen, 2018), but their advantage did not come only from their technology. Israel also put a great deal of investment into research and the development of its people, such as the training of students in primary schools. These students then go on to take appropriate positions in the military during the country's compulsory military service period.

Israel's approach is in line with Herpig (2015), who found that a proactive approach to cybersecurity is the best strategy, and Israel's success highlights the potential for other nations to emulate their efforts (Cohen, 2018). However, while international collaboration can provide substantial advantages of accelerated knowledge, Herpig (2015) claims that the strategy should initially be self-focused. Due to the advantage of possessing superior knowledge, entering a cooperative partnership with the upper hand may allow exploitation of the less informed partner (Herpig, 2015).

Cyber intelligence gathering is a critical step in developing a successful defence. Understanding a potential enemy's plans allows countries to proactively build capable defences (Cohen, 2018); however, along with defensive actions, offensive attacks also require information. The 2010 Stuxnet attack (Lindsay, 2013) used copious

intelligence operations to mount an attack that was targeted at physical property. However cyber intelligence alone was not sufficient, and in this case, physical knowledge was also needed to attack this particular target successfully (Cohen, 2018).

Israel's success in this field raises the potential for other nations to emulate their efforts and this is potentially already underway. Between 2003 and 2013, Israel led the world in investment into research and development; however in 2014, due to a drop in government funding, South Korea moved past them to lead the way (Reuters, 2014). While the Israeli Government continues to invest in start-up businesses and the development of cyber tools, Cohen (2018) notes that Israel's drop to second place in the OECD nations' research spending may impact on their continued excellence in this field. However, this pursuit of a technology-based defence may only form part of an overall defence consideration.

3.9 COVID-19 considerations

The sudden move to remote working that accompanied the COVID-19 pandemic was a reactive measure taken by organisations that were seeking to remain active while doing their best to ensure the safety of their workforce and comply with government orders. For office-based staff, one of the benefits of this was that employees found a new way to save time and costs, as commuting time and travel expenses were dramatically reduced. In these organisations, while business continuity remained high, a new threat was revealed. Organisations' disaster recovery (DR) and business continuity plans (BCP) had been created without knowledge of this potential situation. As a consequence, the threats associated with this new way of working did not receive adequate attention, which meant that each organisation risked having fleets of newly purchased laptops and personal employees' devices (Marczak & Scott-Railton, 2020) that were connected to corporate networks but were less well monitored and sat outside of traditional security boundaries while still connecting to valuable organisation intellectual property and data (Miller, 2020). The outcome resulted in a dramatically increased attack vector landscape that was operating with much reduced visibility for the staff responsible for its protection.

During the pandemic, Deloitte's Cyber Intelligence Centre observed a rise in cyber-attacks, including phishing, malware spam and ransomware (Aladenusi, 2020). The

sudden drive to install and use COVID-19 related applications presented attackers with a greater opportunity to impersonate legitimate vendors in order to gain an advantage. The professional audit firm KPMG suggested that during the disruption, business was initially focused on operational continuity and financial security, but following this initial focus, businesses turned their attention to preparing for the months and years into the future (KPMG, 2020). KPMG presented advice to consider COVID-19 as a point in time from which to pause and reflect on current cybersecurity practices and that the pandemic offered a chance to take a fresh perspective or provide an opportunity for a fresh start for security plans (KPMG, 2020). Professional services and business advisory company PricewaterhouseCoopers (PWC) took a similar view and added that because COVID-19 had driven a greater dependency on technology, the adoption of cybersecurity best practices may have reduced, which may have compounded the problem, as attackers could exploit the changing threat landscape and take advantage of gaps caused by rapid organisational change (PWC, 2020).

From a research perspective, COVID-19 effects were equally problematic. Like corporate staff, researchers were also forced to work from home, which impacted on their ability to complete data collection. Face-to-face interviews and in-person sessions were no longer possible, which in many cases stalled or cancelled research projects (Ramos, 2021). In addition, the publishing process became problematic. The review of manuscripts was delayed, which meant that papers submitted prior to and during COVID-19 took much longer to process, possibly due to the sudden load placed on peer reviewers (Harper et al., 2020; Ramos, 2021). Also, with researchers operating from home, many found more time to write, resulting in an influx of publications (Harper et al., 2020).

The lack of face-to-face contact forced researchers (including myself) to consider alternatives. For this project and others, the ability to conduct interviews via videoconference became an acceptable solution but this did not work for all. Kara and Khoo (2020) found that the digital divide impacted on those whose research projects were less connected to technology. Projects conducted in remote and rural areas often lacked laptop devices and had scarce internet facilities, which reduced the possiblity of traditional vidoeconference methods. However, some reserchers found other solutions and found success using voice or type (Kara & Khoo, 2020).

3.10 Impact of Cyber-Operations

In this interconnected world, traditional physical barriers such as oceans and distance are now easily and rapidly breached by cyber-attack methods, and with the increasing interconnection between virtual and physical environments, any outcomes of virtual attacks will likely have a corresponding increased effect. It is the physical outcomes of these attacks that have captured the attention of social researchers and make this type of research so important. The increase in popularity of IoT devices also increases the ease with which the physical-virtual barrier can be crossed. While the loss of private data, financial resources and consumables may be quite distressing, the loss of computer-controlled infrastructure could be catastrophic and crippling at a country level.

Hacking for fun and exploration has transformed into the cyber-operations of cyber-attack, cyber-espionage and cyber-terrorism, with a mix of motivations from attention seeking to organised crime and state-sponsored objectives. Hacking groups have always shared knowledge and as sophistication grows, detection and mitigation become much more difficult. Consequently, countries are unable to completely prevent cyber-operations such as cyber-espionage, but they will tolerate a level of it before they turn to retaliatory conflict. Then, as countries' conflict levels increase (potentially as a deterrent), they often increase the size of their military; however, cyber-operations increase in frequency as a country's military size expands. This chain of action appears to compound the problem and is potentially self-fuelling. Cyber-espionage or other cyber-operations could be the initial trigger that causes an unstoppable role towards destructive warfare.

Cyber-operations in all forms seem unlikely to stop. There appears to be a never-ending competition between attackers and defenders; however, change brings opportunity, and the COVID-19 pandemic may have become a catalyst for change. The rapid move to remote working created a broader threat landscape with many more vulnerabilities for attackers to exploit, but as attackers continue to test the capabilities of remote network security, defensive teams have begun to improve practices and processes to help remote workers stay safe and efficient. However, while the potential for cyber-attacks to affect physical infrastructure continues, the risk to society is likely to increase.

3.11 Summary

This academic literature review built on the knowledge gained from reviewing practitioner-based cybersecurity literature and began by providing an overview of the creation of the internet. It highlighted the internet's military beginnings and demonstrated the strategy to build in resilience to the internet by design and the ability to use the internet for both cyber defence and offensive initiatives. As is often the case when military objectives accelerate innovation, cyber-operations saw this demonstrated by attacks on physical infrastructure from within the virtual network space. The chapter then reviewed information on the three perspectives of individual, organisation and country, which led to the discovery of gaps in knowledge. Several aspects of the COVID-19 pandemic and how this affected the cyber-threat landscape were included before finishing with a conclusion that brought together knowledge from both academic and practitioner literature reviews to form a more complete analysis of the current state.

This comprehensive analysis of the current literature uncovered gaps that led to identifying the need for further research into how Australian organisations and individual staff consider DDoS as a threat and how they perceive the risks to themselves and their organisations. This research may help to identify improved methods for addressing the likelihood of future attacks of this nature. The next chapter (Chapter 4) details the methods taken to perform this new study.

Chapter 4: Research Methods

4.1 Introduction

This chapter discusses the research methods used in this study to address the research questions stated in Section 1.4.3. The chapter is laid out in a logical order so that readers can follow the aims of the research and methods used to deliver the results detailed in Chapter 5.

Section 4.2 details the research aims so that the objectives of the study and development of the research methods are clearly understood, and Section 4.3 provides details of the assumptions related to the project management process and the DDoS subject matter. Section 4.4 on the research paradigm begins with descriptions of each option available before presenting the final selection and the justification for this choice. Section 4.5 discusses the research methods, detailing the data collection techniques and the data analysis methods, and Section 4.6 describes the questionnaire development process, explaining how each question was developed, the intent behind each section and how the question order was conceived. Section 4.7 on respondent selection explains how the sample pool was narrowed to a workable size, how potential respondents were approached and how those that agreed were screened for interview suitability. The interview style option, the final choice and the reasoning behind the choice are presented in Section 4.8, along with the process used to undertake the interviews and the way COVID-19 influenced the interview process. Section 4.9 outlines the complexity of human research subjects and the study's acknowledgement and awareness of potential research biases. The approach to how these potential biases were managed is detailed in Section 4.10. Associated ethical considerations are discussed in Section 4.11, including the impact of ethics approval controls and how these ethical obligations were met, and finally, Section 4.12 provides a brief summary to end the chapter.

4.2 Research Aims

Research aims are used to understand how best to design the research methods in order to obtain meaningful results that provide responses to the stated research questions. To this end, decisions should be made with regard to whether the research should use a quantitative or qualitative approach and whether it should follow an exploratory, descriptive or causal research design. Prior to any detailed research planning for discovering new insights or building potential hypotheses into the field of study, exploratory research can provide some key objectives. As an open-ended style of research that explores potential options at a high level, it becomes possible to use the observations gained to build a view of potential research directions and the results that may be obtained. In this way, exploratory research can be used to underpin decisions related to further valuable research (Zikmund et al., 2010).

By contrast, causal research design is often used when correlation is the desired outcome; however, undertaking this research design requires a clearly defined situation (Zikmund et al., 2010). This research type could include understanding if an increase in sales staff correlates to an increase in revenue, customer retention or financial turnover. If information can be measured and compared, casual research can be beneficial. While there are some attributes of the study that would benefit from examination of causation, a significant portion of the study seeks to understand the perspectives of organisations and employees; therefore, descriptive and exploratory research designs are more aligned with the majority of this study.

Researchers who are looking for cause and effect results or aiming to understand patterns of results (potentially to predict future outcomes) may also prefer a quantitative approach to make meaningful interpretations of the findings obtained. For example, a question such as “Are larger teams of security experts faster at responding to active DDoS attacks than smaller teams?” could undergo quantitative analysis. Measurements of team size and success rates could be recorded and statistically analysed to obtain results. Also, descriptive research is used to describe objects, including individuals and organisations (Zikmund et al., 2010), and has been used to produce some highly visible research outcomes, such as the quinquennial census of the Australian Bureau of Statistics (ABS, 2021). In these types of studies, descriptive research typically utilises surveys as a method for data capture, but the accuracy of

any projections is directly related to the accuracy of the data gathered (Zikmund et al., 2010).

As DDoS is a constantly evolving topic (Nazario, 2008; Yuan & Mills, 2005) and literature reviews reveal that there is a scarcity of scholarly academic research on the topic, exploratory research methods best fit the criteria required to understand what is meaningful to the research subjects and how they perceive DDoS phenomena, threats and events. Further, as the boundaries of the data collected through interview were not initially clear, grounded theory, a qualitative method that can collect and understand the meaning behind given answers from several perspectives, is included in the research analysis (Bettis et al., 2014).

4.3 Assumptions

This research undertaking can be compared to a project, as its attributes and outcomes (as shown in Table 4.1) align with common project management methodology definitions of what a project is. According to the Project Management Institute (PMI, 2013), a project is *"*a temporary endeavour undertaken to create a unique product, service, or result*"* (PMI, 2013, p. 3).

Table 4.1

Project Attributes.

Definition of Project Attribute	Conforms?	Justification
Is a temporary endeavour	✅	Performed only during the higher degree permitted timeframe
Has a defined start and end	✅	June 2016–June 2022
Must deliver a unique outcome	✅	Research is unique and delivers a unique thesis
Must not have been done before	✅	Each PhD research project is uniquely differnet

Note. Adapted from Murray (2009) & PMI (2013)

Within the project management field, parts of the project can potentially be variable. Project management methodologies refer to a commonly known concept of the triple constraint (Figure 4.1), which states that quality is determined by the relationship of three constraints (Schwalbe, 2014; Westland, 2018).

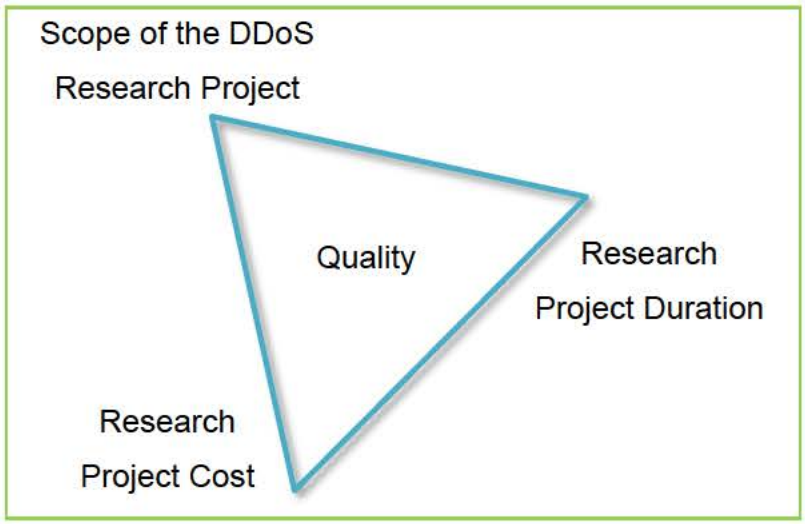


Figure 4.1 Project management triple constraint (adapted from Schwalbe (2014) and Westland (2018))

For example, if this research project is to retain sufficient assessable quality but a shorter timeframe is preferred, then either cost must be increased (such as the use of paid transcription services) or scope needs to be reduced (such as a narrowing of research area). However, many projects have at least one constraint that would be difficult to adjust. Dobson (2004) classifies constraints as:

- A driver - a constraint that, if it fails, also causes the project to fail;
- A weak constraint - the most flexible constraint (not least important), such as the amount of effort (cost) dedicated to the project by the researcher; or
- A middle constraint - which can float between the driver and weak constraint (such as the project scope that can be adjusted).

A project may have two drivers, two weak constraints or a mixture of all three types (Dobson, 2004). The current research project aligns with this thinking as quality needed to remain at the required assessable level and time was considered to be the driver constraint, as failure to complete the research within the maximum time (with acceptable quality) would result in project failure. Cost in this case was considered the weakest constraint; however, there was some flexibility with available funds, as there were several options for attracting research funding if required. Scope was the middle constraint. In this project, while there was some flexibility surrounding the scope, it could not be reduced below acceptable PhD assessable standards (Daniel, 2014) and, as such, scope could not be classed as a weak constraint.

The initial project design needed to consider several assumptions that may be adjusted as more information becomes available, such as the number of available participants, the level of stakeholder support and/or the feasibility of the project goals. Individuals make similar assumptions every day and their daily plans rely on the existence of presumed events that are outside of their control; however, there is enough certainty to allow the individuals to layer pre-determined actions in order to achieve their daily and longer-term goals (Simon, 2011). These may be valid assumptions with various degrees of probability; nevertheless, as more information is uncovered projects make use of feedback loops to determine if follow-on action is required (PMI, 2013). The choice of what to assume often comes from the personal perspective of the assuming person, which is a positivist's point of view, where the actions of the person are shaped by their own historical events (Cicmil et al., 2006; Thompson, 2015), and this affects the assessment of their observations. In the case of a project, this can be the project's leadership (PMI, 2013), and it is this perspective that defines the path of projects and plans, as the assumptions influence relevant decisions and the potential solutions offered as options for selection.

The initial assumptions for this research project were:

1. In the early days of the internet, as shown in Figure 4.2, most attacks were aimed at vandalism with the aim of an instant reward, such as the defacing of a website or the prevention of a service being delivered. Over time, other motivations rose in popularity and in 2018 (Figure 4.2), the gaming industry became the most popular target. Political and criminal motivations also increased and there is now the potential that perpetrators recognise the value of strategically placed attacks that provide longer-term benefits for personal or organisational gain rather than instant rewards. Due to this observed trend, we assumed that strategic attacks would likely increase.

2. Due to the exponential increase of IoT devices being placed in the hands of non-technically aware households/businesses and the fact that these devices are manufactured with a 'price focused' perspective with less concern for device security (Abreu, 2017; Heimdal Security, 2020), we assumed that protecting the potential DDoS source stock would be an impossible task in the short to medium term.

3. As security audit and penetration tests have been aimed at finding weaknesses and gaps in security, such as vulnerabilities in unpatched applications or holes in misconfigured firewalls, and as DDoS works by overwhelming a legitimate entry point with non-legitimate traffic (DDoS attacks do not require access to hidden or poorly protected entrances), we assumed that the general view of IT employees would be that a specific range of DDoS mitigation products and specific DDoS mitigation processes would be required.

4. We further assumed that IT personnel would, if assured of anonymity, be prepared to interview and speak in depth about their personal opinions of organisational and wider perceptions of DDoS threats and mitigation options.

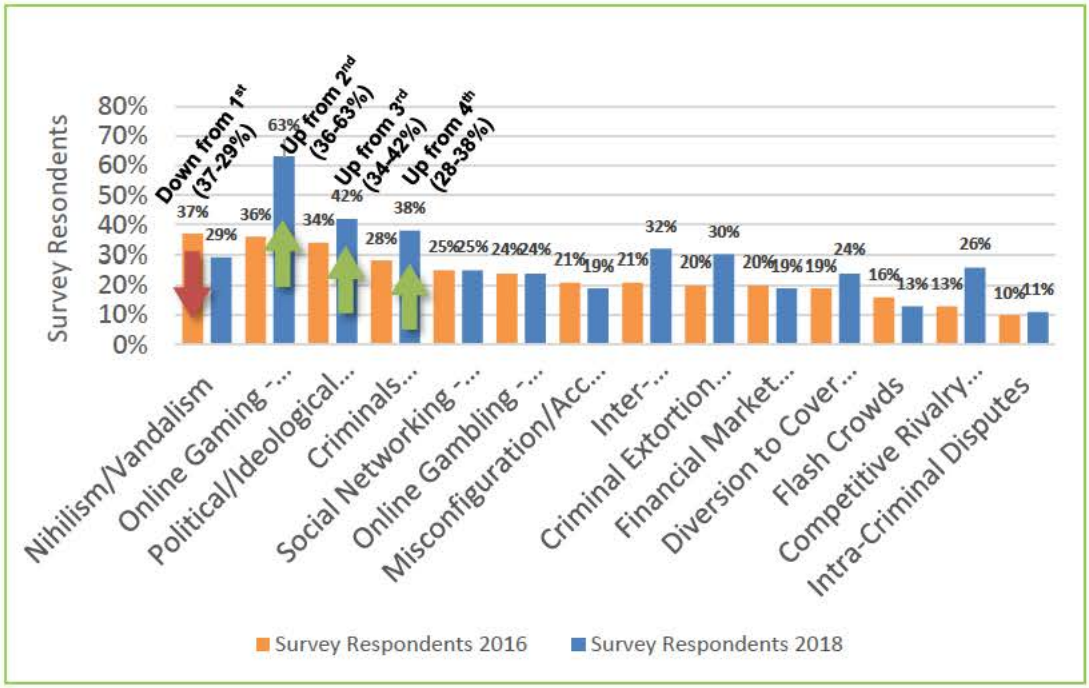


Figure 4.2. Top DDoS motivators 2016–2018 (adapted from Bienkowski (2016) & Netscout (2018))

As the project developed and more was understood about the subject, the assumptions were further developed and adjusted as below.

- **DDoS will be impossible to prevent in the short to medium term**.
  - Whether the source is a legitimate or compromised device, DDoS takes advantage of services that are deliberately configured for accessibility. In effect, an open door that if closed, would effectively prevent all access including that which is deemed legitimate.

- **DDoS as a threat will continue to expand and strategically motivated attacks will become more prevalent.**
  - A consolidated literature review may determine a pattern or trend of attack motivation, which may help to predict future outcomes.
- **Sufficient historical quantitative data are available publicly for analysis.**
  - During the proposal creation, multiple sources of statistical data were discovered. This is assumed to continue.
- **Staff within organisations will be comfortable providing personal opinions of how their organisation, industry and government perceive the DDoS phenomenon.**
  - As data sources were protected and kept confidential, there was a low risk to organisational security and, as such, it was assumed interviewees would be able to respond openly.

4.4 Research Paradigm

By their nature, research projects follow similar rules to projects (in general) and further, according to Kuhn (1970), assumptions can generally be aligned with research paradigms. A research paradigm can set up the context to inform the reader of the perspective from which the researcher observed and analysed their studied material. Lincoln and Guba (1985) offer that a paradigm comprises four elements: ontology, epistemology, methodology and axiology.

4.4.1 Ontology

Ontology discusses the nature of reality and whether the reality perceived by the researcher exists independently or is constructed as a result of individual cognitive comprehension. Ritchie et al. (2014) identify two ontological positions, realism and idealism. Realism states that a philosophical reality continues to exist independently of thought, whereas idealism believes that reality can only exist through belief and understanding (Ritchie et al., 2014). Ontology is important to this project as I seek to understand how individuals perceive DDoS as a threat. This perception may be perspective related, in that the level of threat may change depending on the perspective from which the individual considers the topic. Asking an individual to consider the

threat level perceived by a company requires them to construct a reality from which to answer, and this reality is based on the individual's combination of empirical, authoritative, logical and intuitive knowledge of their organisation. To the individual, the reality from which they answer exists, but from the researcher's perspective, it is a constructed reality that allows the individual to form an opinion.

4.4.2 Epistemology

Epistemology describes the nature of knowledge and how knowledge is perceived from the context of the researcher (Cooksey & McDonald, 2011). Epistemology's question is essentially if knowledge is something that already exists and is waiting to be discovered or whether knowledge is something that is built or newly understood from personal experience. Slavin (1984) identifies four knowledge types:

1. Empirical knowledge – where knowledge is gained through a personal understanding of sensory experiences. A motorcycle racer empirically understands the term 'fast'.
2. Intuitive knowledge – where faith and gut feel are relied on for understanding. A motorcycle appears fast while statically displayed.
3. Logical knowledge – where knowledge is derived from the understanding of theoretical concepts. For example, motorcycle racers aim to win, therefore racing motorcycles are likely to be fast.
4. Authoritative knowledge – where knowledge is received through teaching or reading. Parents advise children that motorcycles are fast.

This project utilised all these forms of knowledge with particular types taking priority at different points in the project. Empirical knowledge was used throughout but was key during the research interviews and data collection. Intuitive knowledge was key in the early stages of the project as it was used to develop the project's research proposal. Little was known about the subject of DDoS perception prior to the project so intuition and intuitive knowledge were used to set an initial goal and an initial starting point for the research. Logical knowledge added value, as logical knowledge allowed several sources of related authoritative knowledge to be used together to corroborate and be accepted as truth. However, authoritative knowledge took priority during the research in the project proposal and literature review stages. At many points throughout this project, authoritative knowledge was gathered and used as a base from

which to build new understanding. It was vital to ensure that trusted and verified information such as peer-reviewed journals and academic texts were used. The understanding of this knowledge helped to form a point from which new ideas could be conceptualised. Overall, combining the empirical, intuitive and logical knowledge that was gained from the literature that was reviewed and the data that were analysed was fundamental to the creative process that led to the production of this distinct thesis, which is based on a unique research project.

4.4.3 Methodology

Methodology refers to the research design and methods, processes and attributes that lay out how the research project flows from start to completion. Aspects of this research project's methodology are discussed at length in this chapter. Methodology could be closely compared to a project plan, as the methodology includes the assumptions, limitations, risk mitigations, scope, and a documented timeline/research plan.

4.4.4 Axiology

Axiology is a branch of philosophy that is concerned with the pursuit of value, with value commonly derived from two classifications: either an object or a human action. Under axiology, an object's value, or worth, relates to the object's aesthetics, such as its beauty, and human actions are considered either right or wrong, with this value being understood as ethics. This project followed the ethical principles laid out by the UNE organisation and upheld by the UNE Ethics Committee (UNE, 2020). Ethics approval for this project is discussed in more detail in Section 4.11.

As this research progressed towards understanding how people perceive DDoS threats, axiology was used to assess the value of that knowledge and whether the outcome of the knowledge attained was knowledge for knowledge's sake (intrinsic value), or whether it could be used to invoke worldly change for the better (extrinsic value) (Hogue, 2011). Axiology is also concerned with the effect of the personal influence of the researcher (Consultores, 2021). Axiology questions if the researcher's opinion affects the way a result is conveyed (Consultores, 2021) compared to a neutral standpoint. Axiology seems to cross paths with epistemology at this point. Axiology questions if the research has intrinsic or extrinsic value, which is dependent on the

values held by the observer, and epistemology questions if the knowledge was constructed or if it already existed independently of the researcher. While the knowledge itself may have some intrinsic value, whether the findings are good or bad depends on the value to the researcher or how the researcher promotes value to their audience.

4.4.5 Research paradigm

Therefore, assumption choice is a vital building block of a research activity, as by understanding the pattern of chosen assumptions, a subconsciously selected research paradigm can be consciously acknowledged and shared (Cooksey & McDonald, 2011). However, even if the research type designates the choice of guiding assumptions, personal bias (Allison et al., 2018) or cogitative dissonance (Mills & Harmon-Jones, 1999) may further influence the final choice, and it is therefore important to discuss and defend the chosen paradigm of research as part of a final submission or published document.

As the choice of paradigm is directly linked to the perspective adopted by the researcher, it follows that a paradigm is essentially a description of the mix of assumptions and preferences of the researcher (empowered to make the selection), and includes their feelings relating to theory in research as well as their opinion of the best methods with which to perform the research (Cooksey & McDonald, 2011). While there are some well-known paradigms such as positivist, which believes universal laws and constants exist (Punch, 2016), or constructivism which believes that reality is constructed locally (Punch, 2016), the number of these "paradigm characterisations" is growing (Shah et al., 2013). As different researchers can apply the same label to different approaches (Neuman, 2006), a clear statement of the paradigm used and the researcher's understanding of the paradigm's definition is a vital inclusion for ensuring that the reader can fully understand the context of the research approach.

To decide which paradigm best applied to this research project, a number of research questions were considered (see Section 1.4.2). In order for the project to address these questions, several assumptions were used to guide and limit the scope of the project. As shown in Figure 4.3, assumptions and project research paradigm choice continued to be developed as initial thoughts and ideas became more mature. The final choice of

preferred paradigm was not chosen during the initial project conception, as unknown and less-understood influences acted to adjust and/or inspire a preferred option. As such, the final paradigm choice considered the ideal paradigm for the developed assumptions, but also involved some bias that reflected the researcher's preference.

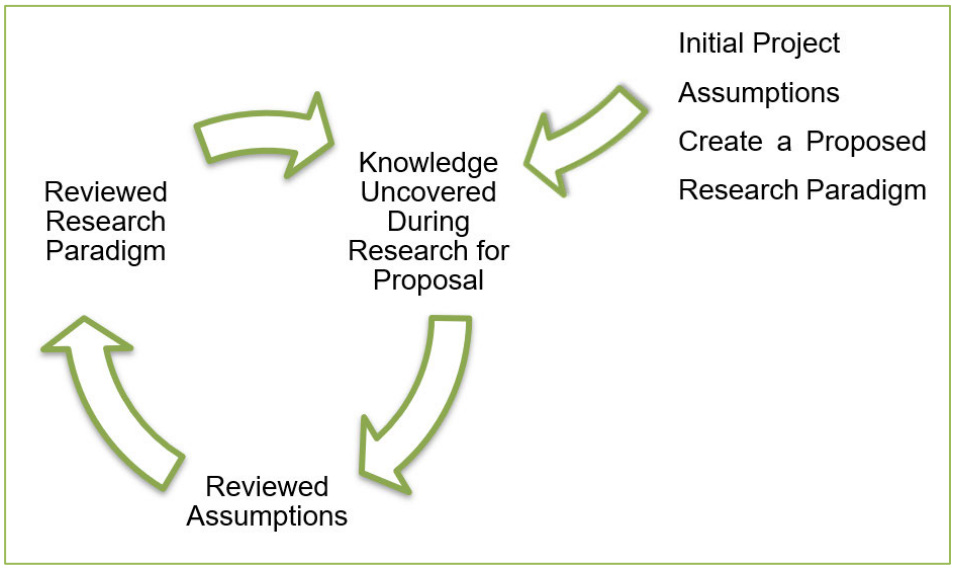


Figure 4.3. Paradigm and assumption development (by researcher)

Of the many paradigms referred to in academic literature, the four most common that scholars refer to are positivism, interpretivism, constructivism and critical theory (Pham, 2018).

Positivism

With positivist paradigms, researchers believe that they can completely separate themselves from their research subject and study the existing results objectively and without personal bias (Hua, 2016; Pham, 2018). From a positivist's point of view, knowledge exists independently and is waiting to be discovered. Also, all that discover it should understand it the same way. Therefore, positivism is often the perspective used when examining numerical data, as there are strict rules surrounding numerical methods of approach and quantitative analysis.

Interpretivism

Interpretivism operates in the opposite way. In the interpretivist paradigm, the researcher seeks to understand the meaning held within qualitative data (Hua, 2016; Pham, 2018). Performing this type of research requires the researcher to create a relationship with the participant so that they can understand subtle points of view;

however, in doing so, they have the ability to impose a bias on the results that stem from their own interaction with the research subject. It is due to this personal influence that interpretivists believe that knowledge is relative and that individuals see the world according to their own interpretation.

Constructivism

Constructivism provides a third alternate view. While positivists believe that the researcher is a passive observer of data and interpretivists focus on how data are interpreted, constructivists believe that individuals play a part in the construction of knowledge (Hua, 2016). In a constructivist's world, involvement with learning allows individuals to shape the knowledge that is learned. For example, two groups may shape the way they view the world differently based on their perceived social structures, such as class and nationality.

Critical theory

Critical theory shares some alignment with positivism as it bases its ontology on realism. However, a researcher adopting critical theory applies their inherent values to their interpretation of the results and also believes their research should be driven by the need to transform, rather than just observe (Pham, 2018).

Paradigm choice

Assessing each of the project assumptions against each element of the four paradigms revealed the logical paradigm choice for this project. Only the first assumption, "strategic attacks would likely increase", aligned with a positivist perspective.

Assessment of the variation (increase or decrease) in strategic attacks is something that can be independently verified through quantitative analysis. These attack statistics will continue to be recorded, with researcher interference and the ability to collect supporting data from independent sources adding support to this assumption and aligning it with a positivist's point of view.

Three assumptions more closely matched the interpretivist perspective:

- Assumption two - protecting the potential DDoS source stock would be an impossible task in the short to medium term.
- Assumption three - the general view of IT employees would be that a specific range of DDoS mitigation products and specific DDoS mitigation

processes would be required.

- Assumption four - IT personnel would be prepared to interview.

Each of these assumptions relies on a personal perspective to interpret the results and arrive at a conclusion. Also, the act of the researcher in collecting and analysing the data may influence the final conclusions. Interpretivist research paradigms are commonly qualitative in nature and utilise grounded theory, action research and heuristic inquiry (Pham, 2018). Rather than using existing theories that may not be a suitable match for the study, grounded theory seeks to develop theories that are formed from data gathered from research participants (Turner, 2021). Moving on from descriptive research, grounded theory takes the experiences and social interactions of participants to develop theories (Turner, 2021) that may form frameworks for this and future studies. Formally, action research is viewed as the act of a professional studying their own practice with a view to developing further improvements (Costello, 2003). Contrary to other forms of research method, action research allows change and research to occur simultaneously (Costello, 2003). Through critical reflection of outcomes, it can also deliver part of a continuous improvement process.

Previous research has been undertaken from a positivist perspective (Chadd, 2018; Kang, Park, Yoo, & Kim, 2013; Monowar, Bhattacharyya, & Kalita, 2015; Vishwakarma & Jain, 2020; Zhou, Jia, Wen, Xiang, & Zhou, 2014), where facts and figures were measured and compared against standards and the previous year's data (Bienkowski, 2016; Netscout, 2018). In contrast, this research did not seek to link cause to effect, but rather sought to understand how people relate to and understand how DDoS affects them and their organisational environments. Each participant would likely have a unique perception of their own and their organisation's comfort level, as well as their own assessment of the effort applied to detect and respond to a DDoS event.

When considering the stated research questions, each of the three questions relies on the participants' understanding of the issue, the understanding of the analysis by the researcher or a combination of both. This research attempts to build a picture of the current environment with little existing reference points of view. Therefore, a logical conclusion was to apply an interpretivist paradigm to the research project and progress using a methodology that aligns with that choice. This decision guided the research

project to use interviews, as these facilitate the use of semi-structured, open-ended questioning that allow the researcher to more deeply understand the perceptions of the participant, help to expose any common themes and identify the influence of factors of age, role, time with company, time in industry or exposure to first party or third-party information. Appendix H contains a consolidated view of all paradigms and theories discussed.

4.5 Research Method

At a high level, the research method used was to first establish a review of the current literature and gather knowledge through secondary data analysis and then gather primary data through interviews and document analysis. For the existing literature, qualitative methods were used to examine literature from professional and technical sources (Hox & Boeije, 2005; Johnston, 2017) in an attempt to understand what is currently known about DDoS, the scale of the threat as perceived by industry and the various methods of mitigation. Then, qualitative analysis (Hox & Boeije, 2005; Johnston, 2017) of the literature from existing academic studies was undertaken to understand previous research knowledge and compare it to current and historical industry knowledge.

While analysis of this literature information continued up to the point of analysis and interpretation, early-stage analysis was sufficient to expose areas of low detail and knowledge gaps from which several research questions were developed (Agee, 2009). The literature review pulled information from books, websites, interviews (video and transcribed), white papers and commercial cybersecurity reports. It also gathered knowledge through digital searches of the UNE library and its affiliates and Google Scholar. This wide range of sources was combined to develop a baseline of knowledge from which to build new understanding of the perceptions of individuals in Australian organisations of the DDoS cyber-threat.

Investigation of existing sources of literature was a fundamental part of this doctoral thesis (Cooksey & McDonald, 2011), as it provides the reader with a consolidated view of existing knowledge, highlights pertinent points and illuminates gaps in understanding (Abrams, 2012; Baker, 2016). It is important that any new knowledge should acknowledge the influence of former peers (Thody, 2011), but the content

produced here is original and complements the existing pool of knowledge (Cooksey & McDonald, 2011). This literature reviews' sources impacted and influenced the understanding of the current state, which led to the discovery of knowledge gaps and the creation of research questions and methodologies (Rewhorn, 2018; Snyder, 2019; Thody, 2011). From this amalgamation of evidence, an output that included one or more of the following three results was gained (Baker, 2016):

1. A practical consensus regarding the topic.
2. A debate that argues one or more opposing perspectives.
3. Gaps in the knowledge due to unknowns or lack of research.

Once written, a solid base from which to structure the methodology for gathering the primary data was formed (Rewhorn, 2018; Snyder, 2019). However, the process of gathering and reviewing literature can be challenging. For this subject, at the time of review there was a vast amount of information available in a wide range of formats. Additionally, it was a challenge for the researcher to understand how deeply to pursue a line of inquiry and how distant to get from the subject in order to sufficiently understand it and its context. Knowing when to stop can be just as difficult as understanding where to start.

For this project, two separate sources of literature were identified. The first source of information was the industry or practitioner perspective. Many companies provide publicly available reports, literature and statistics. Many of these are written by vendor employees in order to encourage action from the reader. The author may wish to influence a change of behaviour or, more commonly, encourage the reader to pursue the remedy provided by the authoring vendor. Some public literature also presents a pure learning opportunity, as some technical experts wish to educate their peers with the new insights they have gained from their own research, while others write to gain professional accolades and celebrity status from being published on popular social media platforms. The second source of information was academically produced literature, which provides a reliable academic view through accuracy-assessed, peer-reviewed papers and journals.

As a thesis can take many months to several years for research and completion (Bendemra, 2013; Patterson, 2016), and the creation of relevant literature is likely to continue in parallel, new literature may become available for inclusion after initial

composition (Cooksey & McDonald, 2011). Therefore, a point (close to submission) at which the review is deemed to be complete needs to be decided (Shultz & Badan, 2009; University of New South Wales [UNSW], 2019). As such, at least during active research, the literature review could be seen as a living document (Shanahan, 2015) that is continually updated while primary sourced data are analysed. It must also be noted that the published findings of other researchers could have a significant influence on currently understood themes (Deschamps, 2018), so care must be taken to include all relevant research up to the point of submission in order to achieve a complete and accurate thesis (Cooksey & McDonald, 2011).

In addition to the literature review, exploratory research was used to deliver primary data where the analysis occurred in two streams that were run concurrently. In one stream, quantitative and qualitative website analysis (Carneiro & Johnston, 2014) was performed to understand the depth and quality of information that medium and large-sized Australian organisations make publicly available. In the other stream, interviews were conducted with employees in medium and large-sized Australian organisations. Initially, the interviews were intended to be conducted face to face, but restrictions caused by the COVID-19 pandemic required an adjustment, so to maintain the Australian Government's social distancing directions, many of the interviews were conducted via videoconference.

4.5.1 Data Collection

Data collection was performed in three phases (Figure 4.4):

- Phase 1 involved the completion of a dual literature review that encompassed literature from both academic and practitioner sources. This divided approach gathered information from the lateral perspective of being outside of the industry (academic perspective) and from inside the industry, which included experienced-based evidence (practitioner perspective), and brought them together to gain a more complete view of the current knowledge.
- Phase 2 collected information from websites owned by a cross-section of Australian industries. Websites were surveyed and assessed against a set of questions that were written to pursue answers to the research questions (Appendix E).

- Phase 3 directly addressed the gaps identified in current knowledge. Employees from Australian organisations that met the criteria of medium and large-sized organisations (ABS, 2010) were interviewed face to face. However, due to the restrictions imposed by the COVID-19 pandemic, face-to-face interviews were mostly performed via videoconference. Employees were interviewed semi-formally using a set of guiding questions that were divided into four sections (Appendix D). Out of 110 requests, 30 interviews were fully completed.

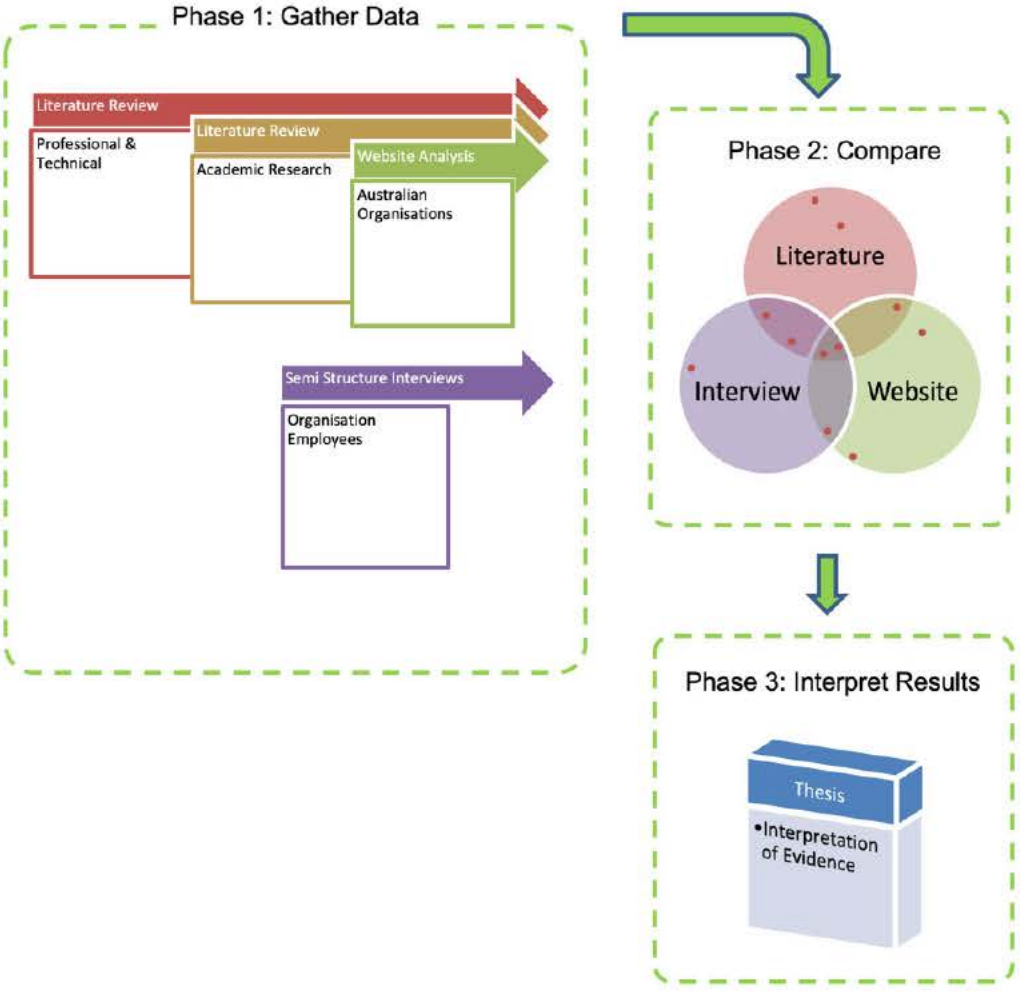


Figure 4.4. Research method (by researcher)

4.5.2 Data Management

Data captured from the analysis of websites was initially entered into an Excel spreadsheet (Microsoft Corporation, 2021) and NVivo 12 (QSR International, 2021). Graphs were constructed using Excel (Microsoft Corporation, 2021) and NVivo 12 (QSR International, 2021), with temporary observations, notes and information being

entered into Word documents and NVivo 12 (QSR International, 2021) qualitative data analysis software.

Interviews were initially recorded using a voice recorder before being transcribed, with the transcription saved into individual Word documents. Each Word document was given a filename beginning with the letter P, followed by a unique number (e.g., P23), to give the file an identifier and obscure the identity of the interviewee to help eliminate researcher bias. These transcriptions were then uploaded into NVivo 12 (QSR International, 2021) for deeper scrutiny, with observations being noted in the Word documents and NVivo 12 (QSR International, 2021). Transcribed voice recordings were erased to make room for new interviews and in line with the requirements for research ethics approval, the transcriptions, along with all other files holding data, were stored on cloud.une for security and data protection.

4.5.3 Participant Interviews

In general, repeatable evidence that can be observed or recorded without bias, either directly (by the main human senses) or by data capture devices, is arguably essential to the validity of research (National Academies of Sciences, Engineering, and Medicine, 2019). Therefore, as discussed in Section 4.6, these questions were put to staff members of organisations that met the ABS definition of medium and large-sized businesses (ABS, 2010) through semi-structured face-to-face and videoconference-enabled interviews. The exploratory nature of the semi-structured interviews (Punch, 2016) was used with the aim of extracting meaning and understanding from key organisational employees. With this primary data analysis, when each participant was asked to give details on future issues and events, they reflected on their own reality and perspective. They then responded with reference to that perceived reality. As it was impossible in this research type to isolate the participant from events and conditions that occurred prior to the start of the participant's observation period, context played an important role. Critically, as each participant responded from their own perspective and point in time disposition, similar organisational approaches were viewed differently, and it was the researcher's role to comprehend and express the relevance of this difference to the outcomes derived.

In Phase 2, qualitative analysis using grounded theory and descriptive analysis that quantified the data were used to analyse, compare and make meaningful interpretations (see Figure 4.4). Analysis of quantitative data was performed to identify trends and anomalies within the pool of data collected, with the data stored and manipulated using Excel spreadsheets (Microsoft Corporation, 2021). Qualitative data analysis was performed initially through manual review and then using NVivo 12 (QSR International, 2021) to detect further insights. Finally, in Phase 3, the analysed information was consolidated (Figure 4.4), and an interpreted review of the results was delivered in the form of this thesis for assessment and for future academic knowledge.

4.6 Interview Schedule Development

Having identified several knowledge gaps, research questions were developed to focus the development of the guided interview questionnaire (Agee, 2009). The gaps identified in the knowledge related to social understanding and perceptive meaning rather than specific technology mechanisms. As such, this study was concerned not only with a respondent's perspective of how DDoS is perceived in their company, their industry and the Australian Government, but also how similar the individual and organisational perceptions are to the widely understood and evidenced supported significance of DDoS.

This research is concerned with the opinions and perceptions that the respondents have formed individually through their interaction with available information, organisational direction, industry influence and the impact of Australian Government regulation/legislation. By undertaking semi-structured interviews where the respondents are guided by pre-composed questions (Punch, 2016), the interviewee was able to deliver their overall perspective of the importance and level of threat of the DDoS phenomenon.

Discussions surrounding the guiding questions permitted identification of thoughts and views that the respondent would potentially not normally consider exposing (Adams, 2015). Unlocking these views was important for extracting the personal perspective from the layer of learned and influenced responses to similar questions that are asked in organisational day-to-day operations. That is to say, an individual often takes on the view of the organisation they represent and masks their own opinion

in order to fit in (Griffith, 2016); however, guiding the interview using pre-constructed questions allowed the research to focus on gathering and understanding a core set of knowledge requirements and restricted the interviewee from straying too far (on a tangent) from the focus of the research.

The data collected came from a mix of respondents from various levels within a company's hierarchy. All respondents were interviewed using the same set of guiding questions so that there was a consistent point from which to assess the various perspectives. The question set (Appendix D – Interview Questions) was divided into five sections:

1. screening questions
2. individual skills and capabilities
3. team skills and capabilities
4. organisation plans and motivation for capability
5. demographic questions

The questions were configured in a thematic order to enable a flow of questioning that better established rapport so that interviewees were more comfortable to answer openly and honestly (Adams, 2015). All questions were intended to be open ended to enable conversation and to allow the respondent to express their views in the manner they found most appropriate (Adams, 2015).

Screening questions

Screening questions appeared first in order to understand the value of pursuing the interview, as a lack of knowledge of DDoS would make discussing later questions very difficult. Statistics were recorded to monitor the quantity of those interviewed and to show the percentage of those with DDoS knowledge and those without.

Individual skills and capabilities

The individual skills and capabilities questions asked the respondent to reflect inwardly and express their level of competence and at what level they perceive DDoS as a threat. Asking the pool of respondents this question was aimed at helping to answer the first research questions:

- How high do organisations rate DDoS as a threat when compared to other

cybersecurity events?

- How is a DDoS threat evaluated?
- Is a DDoS a large threat with low consequence or a low threat with large consequence or somewhere in between?

Towards the end of this section, the respondent was steered towards thinking about recent events within their organisation, which allowed the discovery of factual information and started the shift of focus from inward to outward in preparation for Section 3 about the team.

Team skills and capabilities

The team skills and capabilities questions were developed to investigate employee and organisational competence and to gain evidence for the research question, "Are Australian organisations and their employees aligned with regard to their perception of the threat of DDoS events?" To help this, the participant was asked to reflect externally and examine their perceptions of the teams dealing with DDoS threats and attacks.

The research was still concerned with each respondent's own opinion, but this section shifted the target of focus to team strengths and perceived capabilities along with the mechanics of responding to cyber events.

Organisation plans and motivation for capability

Having discussed team attributes in Section 3, Section four focused on providing understanding for the final research questions:

- Where should effort be focused to ensure Australian organisations are more prepared for a DDoS event?
  - Where should effort be focused (by individuals, organisations, industry and government) to make the DDoS threat more widely understood by employees in Australian organisations?

In this section, the respondent was asked to reflect more broadly and convey their understanding and opinions of how the organisation as a whole considers the DDoS threat. Then, more broadly, impressions of the responsibilities of organisation, industry and government were probed to try to understand what each individual conceived as their preference for utopian cyber defence.

Demographic questions

In the final section, demographic information was gathered to deliver a picture of the achieved data collection pool (Adams, 2015). These data were gathered so the interpretation of results could be built on a data-supported context.

Overall

The structure of the question set moved from a narrow and inward view to a broader and externally facing perspective, with each section building on the information recorded in the previous section (Adams, 2015). By analysing and comparing participants' responses with data collected from literature and websites (Figure *4.4.* 4.4), the project was able to approach understanding the research sub-question of "Is this perception more led by individuals or by organisational culture?" Here, the project attempted to understand the consistency of personal perspectives. Do they remain consistent irrespective of whether the question was asked in a personal, organisational, industry or government context or did the answers sway towards an entity led view?

At all times, in order to maintain confidentiality, organisation and respondent identity was kept anonymous. However, such is the nature of the cybersecurity subject, respondents proved very difficult to secure, which meant the data collection phase was extended beyond original expectations.

4.7 Respondent Selection

As the research project was initially targeting 38 Australian universities, a target of 20 respondents was proposed for interview, aimed at a 50% response rate (Baruch, 1999). Following an increase in the project scope to include medium and large-sized Australian businesses, the number of respondents was increased to 40 so that a deeper pool of data could be collected for analysis. However, in contrast to the assumption that IT personnel would be prepared to interview and speak in depth about their personal opinions of organisational and wider perceptions of DDoS threats and mitigation options if assured of anonymity (Section 4.3) and due to the sensitive nature of the subject, respondents proved very difficult to source. Further, the COVID-19 pandemic (Queensland Health, 2020), which impacted on most of the global population from early 2020, compounded the issue, as it made face-to-face interviews impossible and scheduling interview times through videoconference much more

difficult to arrange. Consequently, aligned with Dworkin (2012) and Galvin (2015) it was agreed to aim for 30 respondents, which gave a balance of achievability and sufficient depth to ensure a solid data base for analysis of primary data.

The respondents were selected from the pool of large and medium-sized Australian businesses (ABS, 2010), with initial selection drawn from the list of Australian Universities listed on the Australian Universities website (universitiesaustralia.edu.au) and later through internet searches for medium and large Australian organisations. Typically, there was no existing direct personal or professional relationship with the organisation, so respondents were identified through existing professional contacts, publicly searchable contact sources such as LinkedIn (https://www.linkedin.com) and publicly searchable company address books (e.g., CSIRO https://people.csiro.au). While potential respondents were prioritised in line with ease of accessing their contact information, a statistical record of contact attempts and results was maintained, and the potential organisation list was periodically examined to ensure a wide cross-section of sectors was maintained.

Each respondent that was selected to participate in the study had a role in an organisation that was likely to be directly impacted by DDoS. Examples of the roles approached are listed in Appendix F. It is acknowledged that this selection process could suffer from the influence of researcher bias, but any unconscious bias was negated by ensuring a wide cross-section of roles was maintained (Appendix G). Roles included in the data collection ranged from frontline support staff who handle customer enquiries to CEOs who are responsible for maintaining business profitability. Impacts on these roles ranged from a direct increase in workload (due to a reaction to control and rectify the outcomes of an attack) to managing stakeholder response, such as protecting the organisation's reputation.

Participants were recruited through direct email or through an email sent to a generic department address requesting participants. In all cases, an information sheet (Appendix A – Participant Information Sheet) was provided as an attachment to offer information to the potential respondent, which gave credibility to the research project and offered the respondent confidence that it was a bona-fide research request. Snowball recruiting (Cooksey & McDonald, 2011) as a method was proposed but only accepted based on the pretext that participants would only be accepted in cases where

the potential participants initiated the contact with the researcher (to indicate their willingness to participate in the project). On acceptance of the research request, face-to-face or videoconference meeting options were presented and a convenient time was agreed. Due to the impact of the COVID-19 pandemic (Queensland Health, 2020), the videoconference interview became the only medium used for the remaining interviews.

The respondents were provided with a consent form to complete (Appendix B – Participant Consent Form) that requested their agreement to be interviewed and recorded. They were also informed that their identity would remain anonymous. The consent form, however, did offer the ability for the respondent to agree to be quoted while keeping their identity obscured. As part of the interview, identifying information such as role, title and length of tenure was only recorded for statistical purposes. Interviews were audio recorded and later transcribed. Recording of the interviews was necessary to ensure that accuracy of the respondents' comments was maintained, as taking notes during an interview raised the possibility of missing comments while writing was performed. Recording also allowed the interviewer to place more focus on each respondent's comments and visual indicators, which allowed a deeper understanding of the intent and meaning behind the spoken words (Adams, 2015). Transcripts were coded with a participant number (e.g., P13) to anonymise the participant.

4.8 Interviews

During the data collection phase, interviews were completed and later transcribed by myself. These interviews were performed using a mixture of physical face-to-face and virtual face-to-face, via videoconference, meetings. Physically performed face-to-face interviews were conducted either at the participant's office or in a local public area. Videoconference interviews were performed with the researcher located at their home office and the participant located at their preferred location (e.g., the respondent's home or organisation's office space). Interviews typically lasted between 60 and 80 minutes and included a preamble conversation that was used to equalise the respondent's and researcher's perceived or assumed level of authority. Preamble

conversations are a method of initiating and enabling a collaborative discussion (Cappellino, 2014; Fontana & Frey, 1994).

4.8.1 Interview Style Options

There are several interview style options, and Fontana and Frey (1994) note three: structured, unstructured and semi-structured. Structured interviewing restricts the respondent to a series of pre-considered responses (Fontana & Frey, 1994) that include questions with options such as Yes/No, Likert scales and questions that permit multiple selection of pre-considered answers like "Choose 3 flavours". One of the benefits of this method is that it reduces the potential for variation that can be induced by the interviewer's influencing bias (Qu & Dumay, 2011). Questions are presented in a uniform manner to all respondents and set a solid base from which to consider the pool of answers. This restricted form, however, presents a limitation in that it is impossible to deviate from the process and pursue deeper understanding of associated meanings that may have contributed to the answers given (Qu & Dumay, 2011). It is therefore possible with a structured interview to gather copious data but miss the question(s) that would deliver the understanding originally sought. Due to its simplicity, the structured interview is well suited to large group data collection, as less time is consumed during the interview process when compared to semi-structured and unstructured options.

Unstructured interviewing allows for a more conversational event and is aimed at understanding the position or perspective of the interviewee. Therefore, a preamble conversation is vital for establishing trust and building rapport (Fontana & Frey, 1994). Questions can occur from both sides (the interviewer and the interviewee), and it is acceptable for the interviewer to allow personal emotions to guide the interview in an alternate direction if they desire (Qu & Dumay, 2011). Unstructured interviews are useful when the knowledge required to develop an accurate question set is not fully understood and a series of unknowns exist (Qu & Dumay, 2011). Therefore, unstructured interviews use open-ended questions that allow the interviewee to use their preferred method to clearly express their opinion. The interviewer is able to adapt and respond to answers and further question points to uncover contextual detail. However, due to the interference of interview flow, it is possible for the interviewer to apply bias towards the interviewee, and the interviewee may fall towards a form of

response bias, such as social desirability bias, where the interviewee adjusts their answer to comply with current social normalities (Börger, 2012). The interview also represents a person's perspective at a single point in time and these can be subject to the influences absorbed by the interviewee up until that point.

Semi-structured interviews are led by a set of guiding questions but allow the interviewer to deviate from the predetermined path if the information received requires deeper understanding. The guiding questions are expected to present a broad theme for the subject matter being probed (Qu & Dumay, 2011). The interviewer presents an open-ended question with a view to engaging in a guided conversation about the subject. Preamble conversation is also vital for establishing trust and building rapport (Fontana & Frey, 1994). Like unstructured interviews, they are useful when not all threads of enquiry are known and understood during the construction of the question set. However, like structured interviews, the respondents are presented with a common set of themed questions that help to build a common base from which to view the pool of gathered responses.

4.8.2 Interview Style Choice

Given that there was little information on the individual perspective, a semi-structured interview style was chosen. At the beginning of the research, there were many unknowns pertaining to what information should be gathered, and the semi-structured interview style provided the ability to deviate from a plan and pursue a line of questioning to discover the respondent's contextual understanding (Adams, 2015).

4.8.3 Interview Process

To establish a comfortable environment, the respondent was able to select a meeting place, format and time of their choice and a short preamble conversation was undertaken to confirm trust and enable open conversation. The respondent in each case was advised of the number of sections and the summary aim of each, which allowed the respondent to understand the path of the interview and allowed them time to reflect and form suitable responses. It also gave an indication of approximate timing and progress through the interview itself, which helped to settle the interviewee and reduce stress caused by insecurity.

The interview was held in an open discussion format where the researcher allowed the respondent to offer their opinion with minimal interruption of what they thought was important regarding the topic (Galletta & Cross, 2013). This allowed the respondent to gain confidence in speaking and offer deeper insight into their knowledge, expertise and experience. All interviews were audio recorded and later transcribed by the researcher (Adams, 2015).

4.9 Research Complexity

When dealing with and interviewing complex human subjects, there needs to be an understanding of how the researcher's perspective can influence the participants' responses. This includes the influence of the researcher performing the interview and the perspective and personal bias that influences and underpins the research analysis (S. Shah, 2019).

On the one side, it is possible that the actions and outcomes of a human research subject could be traced back to a specific cause or influential event. For example, as personal genetics influence many human appearances and traits, antisocial tendencies could potentially be traced to a group of genes. A positivist perspective would consider that the research subjects' outcomes are predictable if enough measurements of subject and environment are collected to become "known" (Hua, 2016; Pham, 2018). Interpretivist researchers take an alternative view, which is that the human research subject has free will to decide and make their decisions based on their continually developed and re-examined interactions and experiences. In effect, they respond independently to the same objective reality (Thompson, 2015).

4.10 Research Objectivity

As interview participants can vary their answers in reaction to past and present influences, it is therefore possible that answers given in an interview environment could be influenced or led by the interviewer due to the participant demonstrating a form of cognitive bias (S. Shah, 2019). Therefore, analysis may additionally be subject to a level of confirmation bias on behalf of the analysing researcher (S. Shah, 2019). It is important to maintain interpretive validity (Maxwell, 1992) through respondent validation (Maxwell, 2012) and ensure what was meant by the interviewee is carried

through to the analysis. Awareness and acknowledgement of these possibilities allowed interview questions to be compiled that reduced these affects (Cooksey & McDonald, 2011). In addition, to ensure descriptive validity (Maxwell, 1992), the transcribed audio recordings were made available to the participants for review. Any inaccuracies could then be clarified and corrected.

Analysis of websites could be considered to be document analysis, as this type of information falls into the categories of public record and media as described by MacDonald and Tipton (1993). Where analysis was performed on websites, the collected data were considered both in context and without context, as interpretation of the information could deliver differing results depending on the perspective from which the information is delivered (Jupp, 2006; MacDonald & Tipton, 1993). This brings a level of triangulation into the analysis (Flick, 2007), which helps to ensure an acceptable quality exists in the analysed results.

Presentation of the results included a degree of discussion, interpretation, observation and implication, which may have been influenced by the researcher. Therefore, efforts were made to distinguish these discussion points from the directly collected data in order to maintain evaluative validity (Maxwell, 1992).

4.10.1 Website Analysis

The combined literature reviews presented an understanding of what is currently known about DDoS within a cybersecurity context, but the literature has been created from the observational perspectives of the authors who examined the historical information, which implies there is a level of separation involved that may result in comprehension inaccuracies and author bias (Palmquist & Connor, 2012). In order to gain an alternate view, website analysis was performed to collate and analyse information that has been published directly by organisations. The websites analysed were those of the organisations of the employees who were interviewed and of the organisations where the employees did not accept the invitation to participate. This method was used so that the results would have a mix of those organisations with employees who were willing to share insights and those who were not, which could expose any differences between the two groups.

As shown in Appendix E, a set of 22 data points were developed. These data points gathered a mix of data types. Eight of the points were quantitative with an exact answer, such as company size and sentence and paragraph counts, and nine had a measurable yes or no answer, such as the existence of live feed or if security training was offered. Understanding these data may reveal any differences between the information larger organisations voluntarily share compared to smaller organisations. Four data points were more opinion based and it is here that researcher bias may have an effect, as the researcher is required to interpret and convey the results. In addition, while the data point regarding security downloads was a yes/no response, this enquiry may also be subject to error as the answer may depend on how deep the download is stored in the website's hierarchal structure. However, analysis that seeks to understand whether the detail type is generic or detailed is more open to researcher bias. To attempt to counter this, when analysing data such as the detail type, these were assessed and reviewed to ensure consistency. The results were initially recorded in Microsoft Excel (Microsoft Corporation, 2021), which allowed a high level of comparison, before being entered into NVivo 12 (QSR International, 2021) for deeper analysis.

The readability of a website may greatly influence readers' understanding of website information (Chan et al., 2018). Where information is of a technical nature, this readability may impact on readers' ability to adopt recommendations and reduce any potential collaboration. Ellimoottil et al. (2012) found that website readability had a dramatic effect on the understanding of a website's information, which is a view supported by Meade and Dreyer (2020), who found that the internet information they studied was at a moderate level and was of less-than-optimal value as the reading level placed it beyond the reach of the average member of the general public. Walters and Hamrell (2008) state that lowering the reading level alone does not aid comprehension, and they found that a lower reading level combined with a reduction in content complexity does aid reading comprehension.

As cybersecurity information is often complex, Flesch–Kincaid tests (Flesch, 1996) were used to compare the readability of both groups of websites. Flesch–Kincaid tests were selected because they are a well-known and widely used readability test (currently the tests used in Microsoft Word). Developed by Rudolf Flesch, the Flesch

reading ease tests aim to provide a measurement scale for readability. A calculation based on average sentence length and average number of syllables per word is used to produce a reading ease score, and this score can be used to predict the grade level most appropriate for the text. The specific formula for calculating reading ease is:

Reading ease = 206.835 - (1.015 x average sentence length) - (84.6 x average syllables per word) (Flesch, 1996)

The resultant output is a number between 0.0 and 100.0, where higher scores indicate text that is easier to read. The Flesch–Kincaid test was further developed to allow a grade level to be determined without the need for conversion tables.

US grade level = (0.39 x average sentence length) + (11.8 x average syllables per word) – 15.59 (Garger, 2020)

The resultant output is a number between 0.0 and 100.0. In contrast to the reading ease score, lower scores indicate text that is easier to read.

Each website had these tests run for the relevant cybersecurity pages with the results recorded in Excel (Microsoft Corporation, 2021). The results were then used to identify any notable difference between the websites in both groups.

4.10.2 Interview Analysis

The analysis of interviews followed an exploratory research process and was performed in two phases. In Phase 1, Microsoft Excel (Microsoft Corporation, 2021) was used to highlight similar responses and identify macro themes. However, due to the mix of quantitative and qualitative data acquired through interviews, Microsoft Excel was also used to analyse Boolean information and the captured demographic data as it provided a simple way to transpose the information into visually comprehensible graphs and charts, which aided understanding. Interviewee identifying information was removed prior to loading the data into Excel, which helped to maintain objectivity in the analysis.

Phase 2 focused on thematic analysis of the qualitative data (Willig, 2013) using NVivo 12 (QSR International, 2021). During the interview process, as the data were collected, uploaded to NVivo and coded, notes of potential themes were included in the journalised notes (Merriam & Tisdell, 2015). These indications were then reviewed as a set to suggest potential themes for inclusion. Then, once the final

interview was completed, the data were reloaded into a new database so that a clean review of coding could occur. This coding was used to identify macro and micro categories across the full interview set of interview data.

4.11 Research Ethics

Research projects within UNE are required to follow the ethical principles laid out by UNE and upheld by the UNE Ethics Committee (UNE, 2020). This ethical obligation exists to minimise potential harm to the study participants and ensure research integrity is maintained (UCL, 2016; UNE, 2020). Ethics approval is generally required as it sets a standard by which all research projects are assessed, but the University of Melbourne (2018a) states that this is not always the case. They advise that in some projects, ethics approval may not be required, such as when using data that have been obtained from public sources or when data collection is through observation of public behaviour. In the case of this DDoS project, approval was required to conduct the interviews as the project was seeking to obtain information that may be classed as personal or private. Ethics approval for this project (Ethics Approval Number HE18-205) was put in place to provide respondents with the confidence that their rights would be protected and they would be treated 'ethically' (UNE, 2020). In addition, it ensured participants that the project would collect data in a way that presented least risk of harm and that their privacy would be maintained.

To ensure ethical compliance, the following actions were taken:

- Respondents were presented with information regarding the study.
- Informed consent was obtained from respondents.
- Participants were advised that they could exit the interview at any time.
- Ethical practices for research, as described by UNE, were adhered to.
- Privacy of participants was protected by:
    - ensuring the confidentiality of responses through data anonymisation.
    - securing data on password protected and encrypted drives.
    - converting any hard copy data to soft copy and storing as above.
- Data will be retained for five years on secure and encrypted storage, after which time it will be destroyed.

On invitation, the research participant was presented with an information sheet (as shown in Appendix A). This sheet, which was based on a UNE information sheet template (UNE, 2019), contained information relating to the aim of the research, how information would be used, protected and disposed of during the project and ethics approval details and information on where to find help in the event of personally upsetting issues should they arise from the interview. This detailed information was required to allow the respondent to make an informed decision regarding study participation. The *National Statement on Ethical Conduct in Human Research (2007) - Updated 2018* states that "consent should be a voluntary choice and should be based on sufficient information and adequate understanding of both the proposed research and the implications of participation in it" (National Health and Medical Research Council, & Australian Research Council, 2018, Chapter 2.2).

This project followed that directive and once committed to interview, the participant was presented with a consent form based on a UNE consent form template (UNE, 2019b) that allowed them to indicate their acceptance of the information provided and their consent to being quoted/published (using a pseudonym) as well as having the interview audio recorded and transcribed. They were also asked to indicate if they would like to receive a copy of the transcription of the interview (Appendix B). To gain UNE ethics approval, copies of the Information Sheet, Consent Approval form and Guiding Questions sheet were submitted for review along with the completed application form. The process for application took approximately 12 days and was returned with a request for clarification in some areas. Clarification was requested for estimates of the length of time requested from participants, verification that data will be retained for a minimum of five years post submittal and information surrounding the destruction of data following the five-year retention period. All the items were addressed over the course of two reviews, and ethics approval was granted on 1 September 2018 (valid for one year). Until ethics approval was granted, no data collection could occur (UNE, 2019b), so this was an important milestone in the project.

Variations to the project can be sought if sufficient change occurs to demand alteration (UNE, 2020). For this project, three variations were sought. The first variation requested the ability to expand the method used to contact potential participants.

Despite several attempts to gain access to staff in universities through mutual and organisational contacts, these efforts were not successful. The requested variation was for approval to contact potential participants whose contact details were publicly available through searchable organisation contact databases. The second variation regarded a change of supervisor and a request to increase the volume of data to be collected. Due to difficulties securing interview participants, an expansion to the field of study from Australian universities to medium and large-sized Australian businesses and a small extension in time were also requested. The third variation was requested due to the COVID-19 pandemic impacting on the ability to schedule and perform face-to-face interviews. This third variation granted an additional 10 months for the data collection phase to allow collection to occur until April 2021. The pandemic prevented further face-to-face meetings, but an option for videoconference enabled the interviews already agreed in the original ethics approval request to be undertaken. A time extension only was sought.

As the interviews conformed to a semi-structured interview style, the questions (Appendix C) were conceived to be open-ended so that discussion of the topic could be recorded and deeper understanding of the participant's perception of DDoS could be acquired. Following completion of the interviews, the content was transcribed and stored securely as per UNE ethics requirement (UNE, 2020) on UNE's cloud storage platform cloud.une (UNE, 2019a). Cloud.une was provided through software from the ownCloud project (OwnCloud, 2020), with UNE's environment providing 500 Gb of password-protected and encrypted storage (UNE, 2019a). Only the documented research team members had access to the data. The plan for data retention was that data should be retained on cloud.une for a period of five years past the submission date. This data will be destroyed five years post completion by the primary supervisor.

4.12 Summary

This chapter covered the research methodologies considered for the study, the reviewed paradigm options and the reasoning behind the eventual selection of exploratory research. The data sampling framework was detailed, including the sample size, method of invitation and screening for suitability. This was followed by a description of the questionnaire development and details of the analysis methods using

appropriate tools Options for interview styles and the logical reasoning for the choice were discussed, including how the COVID-19 pandemic limited available options for face-to-face interviews and narrowed the options available for the semi-structured interviews undertaken. The application for ethics approval was included as it is a necessary step prior to data collection, but also to note the changes required as the pandemic restrictions forced changes to the initial interview plans. Several elements of the process did deviate from the original plan, such as interview format and time allotted for data collection; however, despite the restrictions, data collection and analysis were completed inside the formal limits. The results of the analysis are described in the next chapter.

Chapter 5: Results

5.1 Introduction

This chapter presents the results of the study and addresses the research questions stated in Chapter 1, Section 1.4.2. In addressing these research questions, each area of study is linked back to the existing literature to determine whether the findings obtained from this study support what is commonly known or whether new knowledge or changes have been discovered. Section 5.2 briefly describes the major themes identified during the literature review and highlights the gaps in knowledge that contributed to the development of the research questions and drove the acquisition and analysis of the data in this research. In Section 5.3, the website analysis and observations are first outlined, then the micro thematic categories of relevance that emerged are analysed in depth. These findings support the need for this research and the lack of existing information in this area. In Section 5.4, the results of the data collected from interviews with employees of Australian organisations (Appendix G) are presented, including a descriptive analysis of the demographic results, the observations made and the comparisons between the demographics of the analysed groups and the existing themes collected during the dual literature reviews. Finally, Section 5.5 describes the demographics involved with this study.

5.2 Identification of Research Themes

To provide a framework to assess the results of the website analysis and semi-structured interviews, data were grouped into thematic categories based on the literature review, as described by Clarke & Braun (2017). This grouping brought initial order to the complex set of information and clarified the overarching themes. Seven macro themes were identified in the literature: approach, communication, method, motivation, risk ownership, risk and threat. In some cases (see Table 5.1), these macro themes had already been reviewed in the existing literature; however, this study added new findings, thus making an original contribution.

Table 5.1

Macro Themes in Existing Literature

Theme	Reviewed in literature review		
	Academic	Practitioner	New Knowledge
Approach	✓	✓	✓
Communication		✓	✓
Method			✓
Motivation	✓	✓	✓
Risk Ownership		✓	
Risk	✓	✓	✓
Threat	✓	✓	✓

5.2.1 Macro Theme – Approach

The ‘approach’ macro theme captured information about how organisations and employees approach cybersecurity defences; that is, whether the approach is ‘strategic or tactical’ or ‘proactive or reactive’. The practitioner literature review revealed some thoughts on the benefits of information sharing, but also that this sharing is undervalued by managers (Brilingaitė et al., 2022). In general, the practitioner literature focused on technology solutions, whereas with the examples of Israel and South Korea jostling for leadership in cybersecurity investment, the academic literature offered insight into countries’ strategic plans for technology innovation and also provided information on the human side with education and personal development (Cohen, 2018; Reuters, 2014). However, there was little information in

the literature that was directly from the organisations themselves, so an opportunity to improve this knowledge was presented.

5.2.2 Macro Theme – Communication

This theme includes how organisations communicate both internally between staff groups and externally with customers, vendors and other stakeholders. For development, the practitioner literature showcased that attacking groups have used communications to advance their capabilities through the sharing of knowledge (Kizza, 2017). However, this sharing of knowledge is much rarer in businesses, with little information available from businesses detailing the effects during and after a DDoS attack. At best, an organisation may publicly note a data breach or a reduced performance event, but the detail, facts and statistics tend to be presented by third parties that offer their own analysis of what can be observed from a public perspective. This research project had the opportunity to investigate further and uncover new knowledge.

5.2.3 Macro Theme – Method

How an organisation defines, designs and implements their cybersecurity response was not found in the practitioner literature. The academic literature offered various theories of motivation (McClelland, 2010; Rogers, 1983; Tanner & Raymond, 2012) but it stopped short of detailing the methods organisations have used in the real-world environment. Similarly, while organisations may promote their compliance with cybersecurity standards (e.g., NIST, ISO 27001), they do not offer adequate explanation of the method of implementation. As such, another gap in knowledge was identified.

5.2.4 Macro Theme – Motivation

The motivation macro theme considered both attack and defence motivations. The practitioner literature review revealed information on individual motivators, which range from exploration and fun as different methods of cyber-attack (including DDoS) were discovered to the activism, criminality and state-sponsored motivators seen today. The academic literature added to this knowledge by presenting knowledge on how culture and a country's political structure influences how it seeks to apply its cybersecurity capabilities and its potential to be a victim or aggressor. However, while

information related to motivations for attack were found quite readily, there was little information regarding motivations for defence, and little information was present to describe what drives individuals and organisations to decide on their chosen defence strategy. This is therefore a gap in the existing knowledge.

5.2.5 Macro Theme – Risk Ownership

When a risk is identified, organisations have four options with which to respond: avoid, reduce, transfer or accept (PMI, 2013). The practitioner literature discusses how this choice is determined, explaining how it relies on factors such as organisation size, relevant regulations, existing capability and the consequence of the risk itself. Businesses without infrastructure expertise (e.g., SMEs) may seek to transfer the risk to a vendor or supplier, whereas larger organisations may prefer to mitigate in-house, owning or accepting the risk while fully controlling the management of the event. Regulatory requirements may force avoidance such as the risk of fines or other penalties; however, if the risk is small in comparison to the reward or the risk is deemed a necessary action to conduct business, acceptance may be the only option available.

5.2.6 Macro Theme – Risk

In this thesis, the 'risk' and 'threat' macro themes were separated. They tend to be commonly confused; however, threats are the methods of exploiting a vulnerability, whereas risks refer to the likelihood and consequence of the threat occurring. Both the academic and practitioner literature agreed that the risks of a DDoS attack occurring are increasing. The practitioner literature states that the frequency of attack continues to increase, (ACSM_Admn, 2019; Campbell, 2918) and that the increasing rate follows the acceleration of improvements in DDoS-capable technology (Hulme, 2019; Jackson, 2019; Korolov, 2017; Rayome, 2019). The academic information shows that risk may change within countries as factors such as GDP and military size fluctuate over time, and therefore an individual's risk assessment could be influenced by the culture they are immersed in. As humans are considered to be the weak link in cybersecurity (Wiederhold, 2014), how they respond can have particular influence on the resulting consequence. However, this information comes from sources that have analysed organisations' security posture from an external perspective rather than the

perspectives of organisations employees. As such, through direct access, this study can add new knowledge in this area.

5.2.7 Macro Theme – Threat

The ‘threat’ macro theme covers the types of threats that fall under the banner of cybersecurity. The practitioner literature raised the issue of the role that IoT devices play in facilitating cyber-attacks (Woolf, 2016) and the potential for this to increase as IoT popularity increases. This literature review also recognised the role IoT plays in infrastructure control systems, highlighting that in this traditionally functionally focused area (Song et al., 2017), which operates over LPWAN technologies (Torre et al., 2021), security may be a second thought, and this could lead to critical infrastructure interruptions. The academic literature sees humans as a credible threat, given the propensity for human error. Also, as humans are open to manipulation through social engineering and they are vulnerable to factors that influence their accuracy, it increases the likelihood that even the most well thought-out defences could be compromised by a human miscalculation or action. The academic literature also identifies that many indicators of an attack do not trigger the human senses, which can amplify the threat unless specific monitoring capabilities are implemented. The practitioner literature presents thoughts from a high-altitude perspective, and the academic information presents similar high-level perspectives about how groups may behave when faced with common threats. However, little has been written from the perspective of the employees who face the threats on a day-to-day basis, or how their organisations rate the credibility of the threat. Therefore, this study can add more value to this area.

5.3 Website Analyses

To gain an understanding of how Australian organisations rate DDoS as a threat, the websites of the organisations approached were examined to compile information on their security perceptions. This included the websites of organisations of employees who were interviewed and those organisations where the employees refused the invitation or were unable to respond to the request sent out by the researcher. As a website acts as a medium for the company’s public information and is a method for

facilitating communication, knowledge gathered through website analyses was logically categorised within the communications macro theme.

Of the 48 websites sampled (Figure 5.1), 48% (23) did have some cybersecurity information, but the remaining 52% had no publicly available cybersecurity information. Further, of those websites with cybersecurity information, the security aspects were indistinct and difficult to find. For example, on one site, it was difficult to navigate to the cybersecurity information as it was located three levels from the root of the site and followed a less than logical path (e.g., it was necessary to navigate through governance then leadership information before finding the cybersecurity information). In most cases, the cybersecurity information was found using the website's search functionality. These website searches revealed that security information was mixed in the results categorisation. For example, some information was in the form of product information (where the website belonged to a cybersecurity vendor) and others had published cybersecurity policies that were aimed at the organisation's employees and clients, which revealed that internal education was a priority for the organisation.

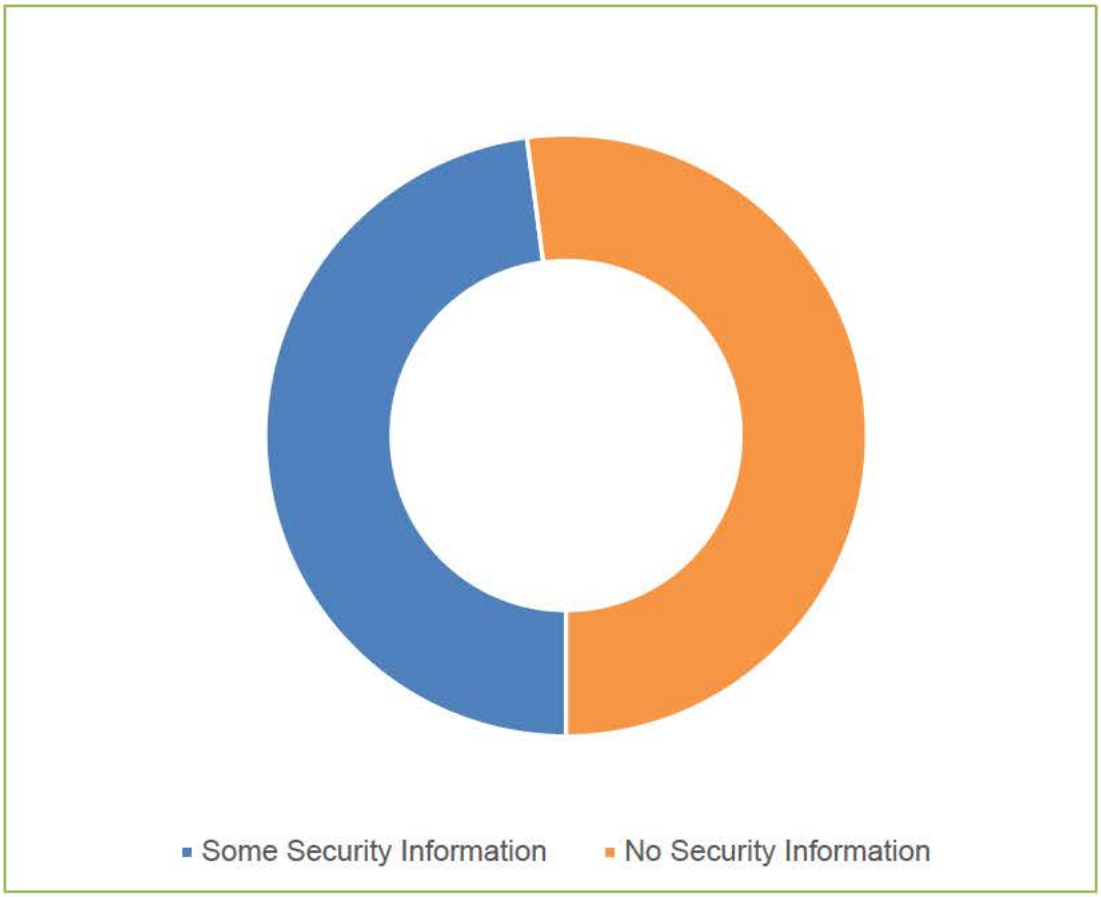


Figure 5.1. Security information on websites

This lack of availability of the information was in contrast to the websites' privacy statements and terms and conditions, as all of the reviewed websites contained a prominent link to this type of information. Under Australian consumer law, all Australian websites are required to display terms and conditions (Australian Competition and Consumer Commission [ACCC], 2021), and for organisations that collect any customer or visitor information, privacy statements are mandatory (McKee, 2021; Office of the Australian Information Commissioner [OAIC], 2021a). However, there are no current legal requirements to include cybersecurity information in the terms and conditions. Any information shared is done so voluntarily and any organisation that does so has likely been driven by organisational objectives. In the website analysis, the cybersecurity information that was offered was low in detail; however, 8% of the websites did offer white papers as a downloadable option. Only 5% offered end users the option of cybersecurity training.

Where cybersecurity was mentioned in the sample websites (48%), the information was covered in a mean average of 17.3 paragraphs, which encompassed a mean average of 18.7 paragraphs for the websites of those interviewed compared to a mean average of 15.3 paragraphs for the websites of those who were not interviewed (Figure 5.2). Of the total number of websites reviewed, the mean average paragraphs dedicated to security was 8.2, but this included the 52% of sites that did not show any security information at all. Of the examined websites that provided cybersecurity information, 56% were interviewed, and this group provided the largest average of cybersecurity information.

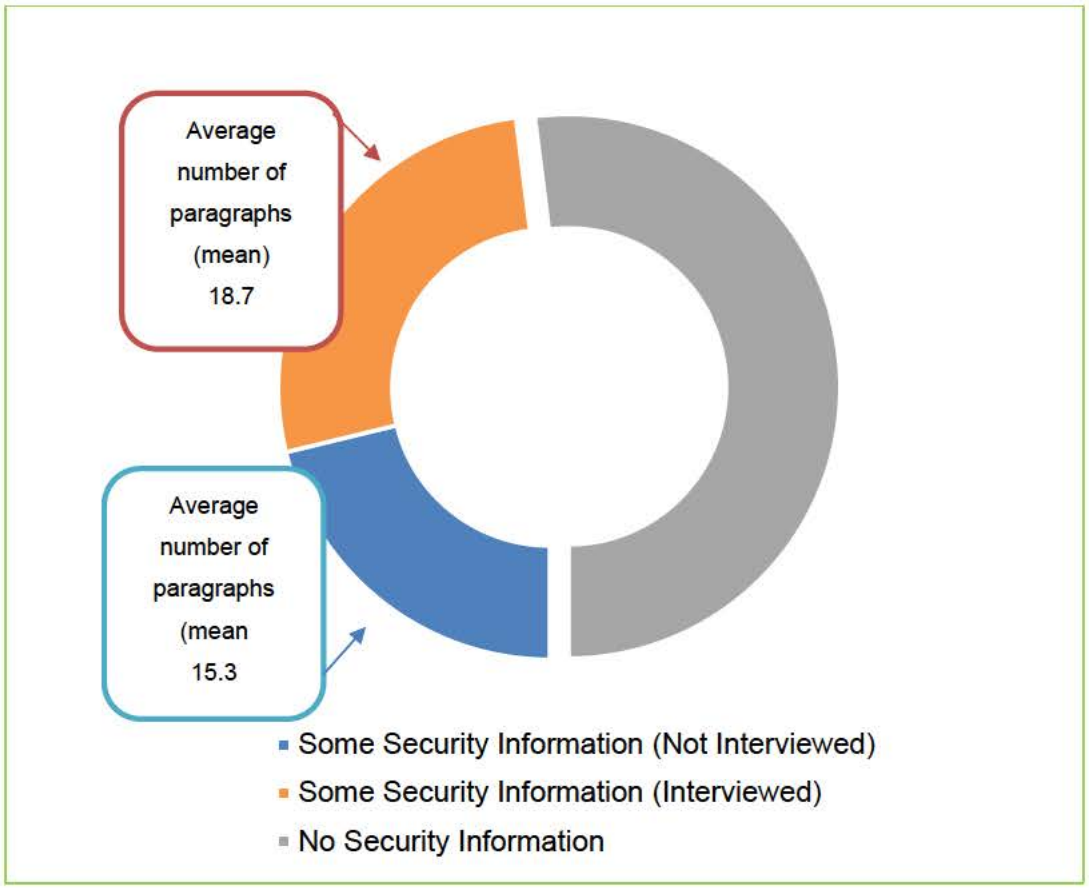


Figure 5.2. Website paragraph counts

Examination of sentence count showed slightly different results that were much more comparable (Figure 5.3). Where cyber-security was mentioned in the sample websites (48%), the information was covered in a mean average of 37.65 sentences overall, with an average of 37.69 sentences for the websites of the organisations of the employees interviewed compared to a mean average of 37.6 sentences for the websites of the organisations where the employees were not interviewed. Of the total number

of websites reviewed, the mean average sentences dedicated to security was 18.04 when including the 52% of sites that did not show any security information at all. This analysis shows that each group (interviewed websites and not interviewed websites) present, on average, very similar quantities of sentences related to cybersecurity, but paragraph structure and page layout differ.

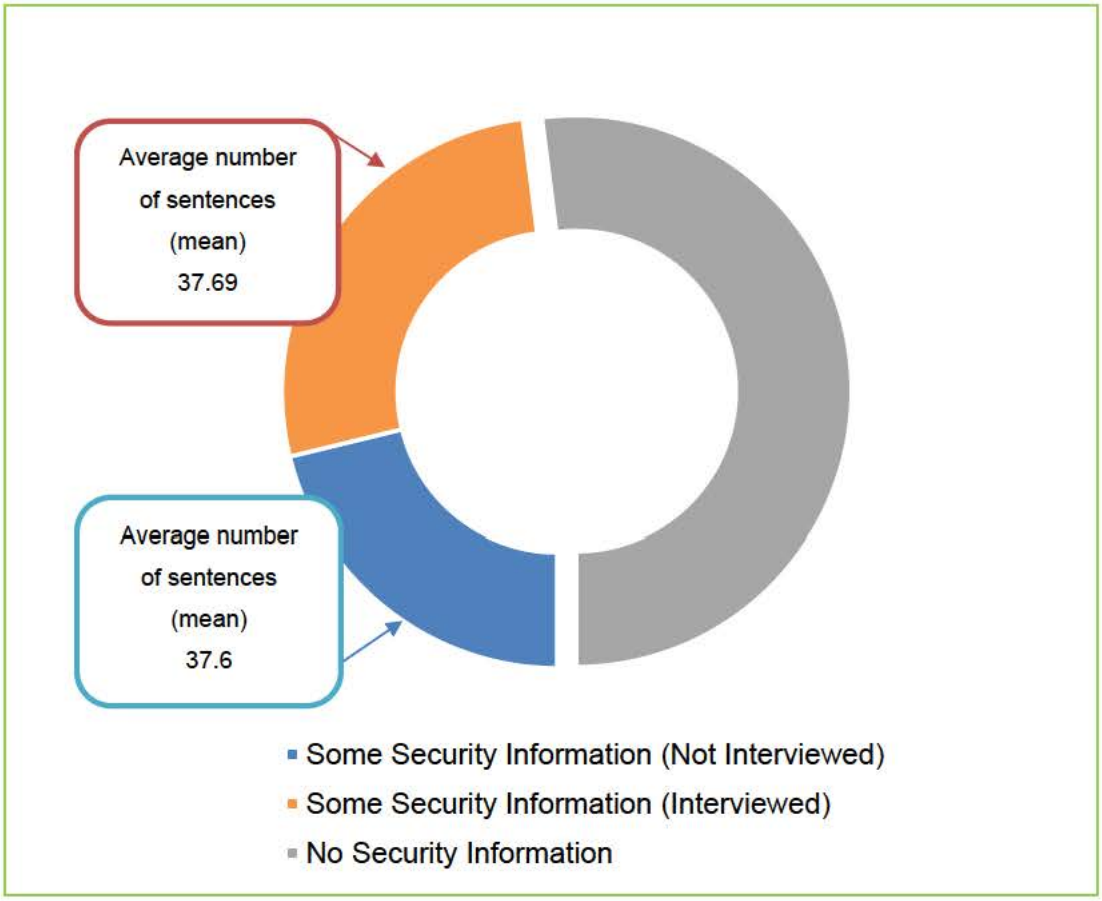


Figure 5.3. Website sentence count

The presence and quantity of images on a website can influence how information is laid out and hence affect the structure of informational text; however, analysis of the sample pool of websites showed that despite 56% of the websites providing information about cybersecurity, as shown in Figure 5.4, this information was rarely supported with images and diagrams. Images and diagrams are often used to aid understanding of complex technologies, and without this assistance, written text may need to be simplified to facilitate comprehension. To this end, Flesch–Kincaid readability tests were performed on the websites to assess if there was any noticeable difference in the level of written complexity between the two groups.

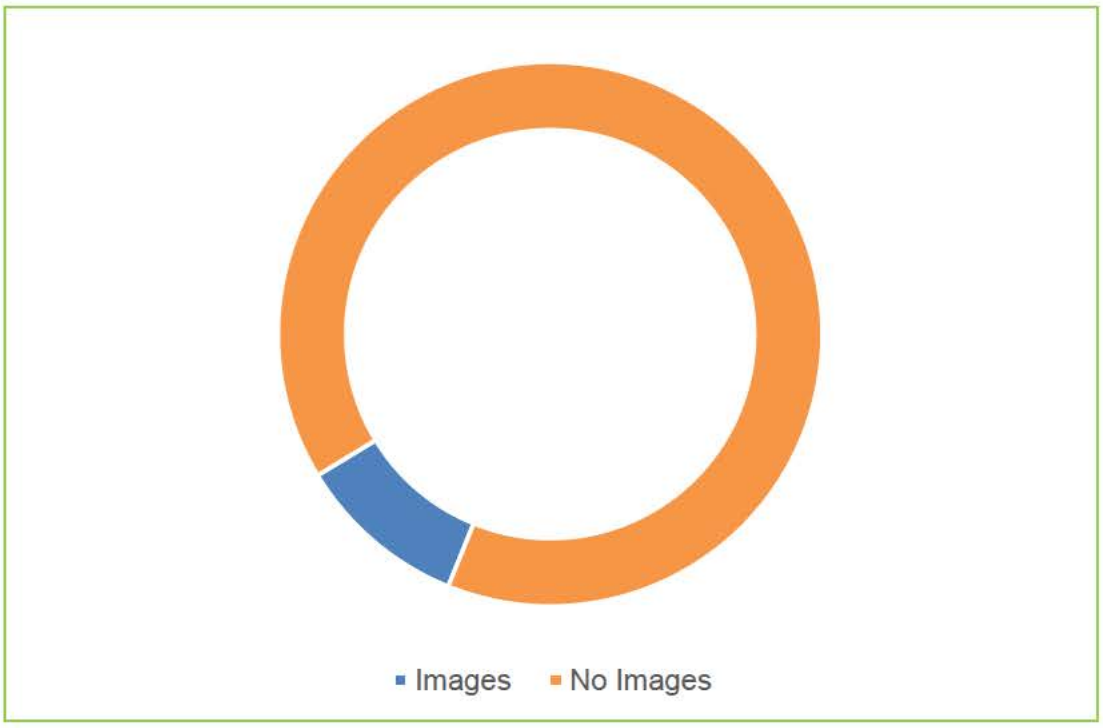


Figure 5.4. Websites showing supporting images and diagrams

Table 5.2 shows the mean averages of the results from the sample websites. On average, those websites with no security information were easiest to read. For example, the website with the highest recorded level in the sample pool had no display of any cybersecurity information and was assessed to have a reading ease of 70.4, which equates to a school grade of 4.7. This means that the information on this website should be able to be easily understood by students in Grade 4. This reading ease is much lower than the website with the simplest cybersecurity information, which had a reading ease of 50.4 that equates to a school grade of 7. However, of the websites with cybersecurity information, it was the websites of the organisations where the employees were interviewed (on average) that used language that could be understood by lower school grade audiences. Thus, there could potentially be a link between a willingness to present easily understood cybersecurity information and a willingness to be interviewed and share their thoughts on cybersecurity.

Table 5.2

Flesch–Kincaid Readability Test Results

Measurement	Reading ease	Measurement	Grade level
Mean average of all analysed websites	39.68	Mean average of all analysed websites	9.47
Mean average with security information	34.37	Mean average with security information	10.30
Total mean average of interviewed	33.75	Total mean average of interviewed	10.27
Highest score of interviewed with security information (easiest to read)	50.4	Lowest grade of interviewed with security information (simplest)	7
Lowest score of interviewed with security information (most difficult to read)	22	Highest grade of interviewed with security information (most complex)	13.1
Total mean average of not interviewed	35.19	Total mean average of not interviewed	10.35
Highest score of not interviewed with security information (easiest to read)	47.5	Lowest grade of not interviewed with security information (simplest)	7.6
Lowest score of not interviewed with security information (most difficult to read)	19.2	Highest grade of not interviewed with security information (most complex)	17.1
Total mean average of websites with no security information	44.56	Total mean average of websites with no security information	8.70
Highest score of no security information (easiest to read)	70.4	Highest grade of no security information (easiest to read)	13.4
Lowest score of no security information (most difficult to read)	21.6	Lowest grade of no security information (most difficult to read)	4.7

Overall, as shown in Figure 5.5. there was a larger number of websites, at the Grade 8 level, that omitted cybersecurity information. This contrasts the grade 10 websites which showed greater numbers of websites with information on cybersecurity.

Figure 5.5. Comparison of website readability by Australian school grade

With approximately 50% of the sample pool sharing or promoting cybersecurity awareness and information, user interaction abilities were investigated. Examination of the ability to observe the current state of cyber-threats or incidents in the sample pool of websites highlighted a lack of live feeds, logs and blogs. None of the websites in the sample pool displayed a live feed or incident log and only 4% shared a blog. It is therefore difficult to identify if an organisation has previously been the victim of a cyber-attack. Large and notable attacks do gain publicity, especially if the target is a well-known organisation. These organisations notify their customers of intrusions that may affect the security of their personal and private information (PPI) and/or their payment card information (PCI), and if these notifications are reported by news organisations, they remain in the public domain for future knowledge. However, if they are not reported and published by a third party, this information disappears over time and may not be advertised by the victim's publications.

Also, only one organisation listed their publicly reported incident, which was confirmed by an intensive internet search for correlating reports. A similar internet search was then performed for the rest of the sample pool but no publicly listed information on cybersecurity incidents was discovered. While legislation mandating the reporting of cybersecurity breaches came into effect in February 2018 (OAIC, 2021b), not all cybersecurity incidents are reported as the legislation only covers private and public companies with turnovers greater than AUD3 million and only

those that need to comply with the *Privacy Act 1988*. Even so, while reporting may be mandatory for some and affected customers are required to be notified, there is little in the legislation to encourage or enforce public notification of all cyber-attacks. Further, while the OAIC has several years' worth of cyber breach reports, it does not name any specific organisation and carries no information about DDoS attacks. As a result, many of the DDoS attacks that do occur fail to be publicly acknowledged by organisations and even less are newsworthy enough to gain the attention of the journalists, whose publications could help maintain the durability of the new event for historical comparison.

Therefore, the websites were analysed to determine if there was any ability to report a discovered incident and if this reporting ability could occur in real time (e.g., instant message/chat option) or via another asynchronous communication method. In 33% of the websites in the sample pool (and 60% of those that carried cybersecurity Information), there was a process to report a security incident (Figure 5.6). Methods of reporting varied. Some requested contact be attempted via phone or email while others presented a web form for the reporter to complete. In 10% of the sample pool (and 35% of websites that share security information and have a method of reporting), individuals were directed to use a portal that required existing account authentication. This process is limiting, as in these cases, only existing employees or customers would be able to raise an alert regarding an incident. However, this process has the advantage of reducing the likelihood of bogus reports being submitted.

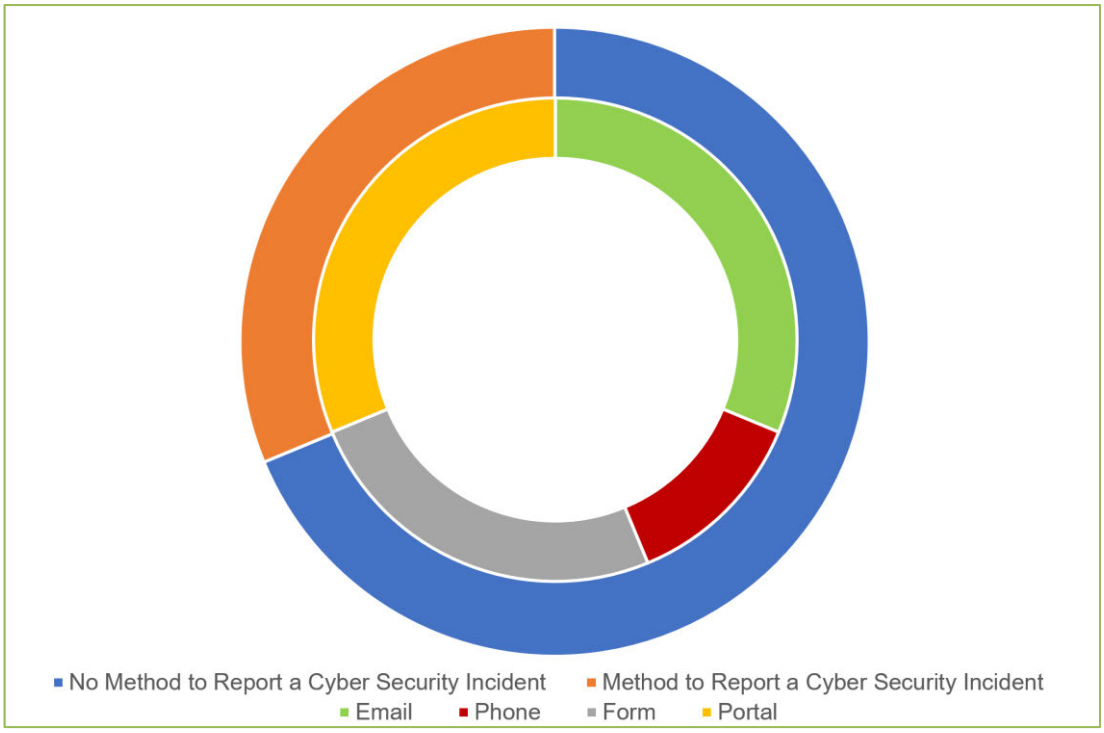


Figure 5.6. Website's ability to report a cybersecurity incident (with reporting method)

Only 5% of websites utilised chatbots/artificial intelligence (AI). This was a surprisingly small number as many previous reports indicated an accelerated adoption of this technology, with some predicting that by 2021, up to 85% of customer interactions would be handled without human interaction (Jovic, 2020; Marriott, 2011). This may be due to adoption rates in Australia. While 65% of brands in the USA use chat, only 4% of brands in Australia use chat (Dilmegani, 2021). The low adoption could be due to concerns about security, lack of local expertise and a lack of executive support due to vague business cases (CX Central, 2020). These security concerns are a result of the lack of knowledge and lack of maturity of the technology (Rajasekharaiah et al., 2020), but also rests on the lack of capability in the workforce, which is relied on to initially implement the technology and then apply substantial effort to develop its ultimate capability (Gekara et al., 2019). Without a specific method to communicate a cybersecurity event, consumers may need to seek alternative contact methods. These methods could include email or phone but would only be possible if enough accurate contact information were accessible on the website and may discourage a consumer from reporting at all.

Around 58% of the sample pool of websites had a generic ‘contact us’ delivered via web form. Web forms are often preferred over the HTML mailto: command due to the ease with which bad actors can programmatically gather email addresses from webpages and go on to utilise them inappropriately, such as for SPAM mailouts. Web forms also allow the website owner to control the information gathered by either limiting the type of information or making some information mandatory. This combination of controls allows a website owner to improve the quality of the contact communications they receive. The downside of this method for the consumer is that they do not always get to send the information they may feel is relevant and they may not always retain a copy of the information they send.

Approximately 60% of the websites provided email and phone details, and in some cases this was provided alongside the web form. In the majority of cases, this email and phone information was highly generic in nature so information sent would have to transfer through the organisational communications path to reach the intended recipient. Staff directories are usually present on internal networks but in the pool of websites analysed, just over 8% had a staff directory that is exposed to the public internet. Some allowed easier search capability than others. In some cases, names needed to be known before a search could proceed; however, in other cases, it was possible to search on a wildcard of a role title. For example, searching for ‘chief’ found COO or CISO and searching for ‘security’ discovered both cybersecurity and physical security contact details. Despite this ability on some sites, it was observed that most sites listed general contact details and advertised the names of the executive teams, making special reference to their background and experience.

Overall, as shown in *Figure 5.7.*, contact methods were consistent across all websites analysed irrespective of whether their employees were interviewed or not.

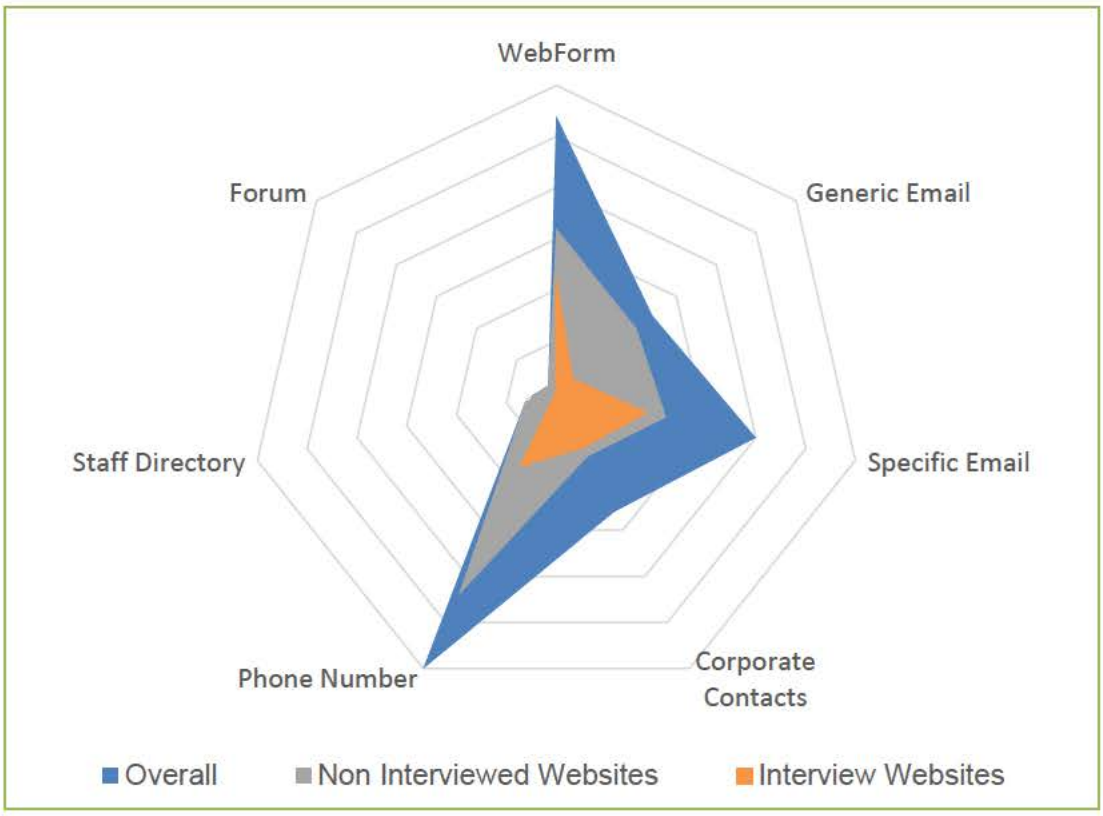


Figure 5.7. Website contact methods

Finally, the websites were reviewed to see if there was any information related to strategic security partnerships. Notification of a partnership may indicate a preferred method of protection and endorsement of a provider's capability. In the sample pool, listed partnerships were rare. Only one website linked to the Australian Government's 'Scamwatch' program. Where others contained a link, these links were to partners who did not operate in the security sector. There was no information about security partnerships. Very few mentioned any of their partners and, where they did, security partnerships were not included.

5.4 Interview Analysis

Following the analysis of websites, 30 employees from medium and large-sized Australian organisations were interviewed to gain a deeper understanding of their cybersecurity perceptions. Following the qualitative analysis performed using the methods detailed in Chapter 4, Section 4.10.2, the seven macro themes of approach, communication, method, motivation, risk ownership, risk, and threat were identified.

Deeper analysis of the interviews revealed important micro themes, which are discussed in the sections below.

5.4.1 Approach

Participants approached cybersecurity with several considerations. From one perspective, they looked internally and took ownership of the risk, considering where they should place effort in the defence of their organisation. For DDoS, some participants (33.33% (n=10)) reported that their organisations had a specific plan, whereas for others (40% (n=12)), DDoS defence was included as part of a more general cybersecurity plan. The rest either had no plan (10% (n=3)) or did not know what the organisation was doing (16.66% (n=5)). Where plans were in place, the approach could be strategic or tactical, with strategic approaches more common (50% (n=15)) than tactical (25% (n=6)). There was no detectable correlation between the choice of a strategic or tactical approach and the resulting plan (DDoS specific or general cybersecurity defence). Strategic plans mostly aligned with proactivity (Table 5.3); however, when considering motivation, reactive plans were produced by organisations that have been previous victims. Three participants reported that their organisations had outsourced, leaving their cyber defence in the hands of ISPs or their cloud vendor. Three admitted that their organisations had no plans in place to mitigate DDoS and a further four were not aware of any plans.

From another perspective, organisations looked externally and saw benefit in consumer protection. The introduction of standards could see Australian and international technology being held to a common level of defence quality, which would level the competitive field for manufacturers of internet-connected hardware and software, and provide Australian businesses and consumers with a minimum level of protection.

Table 5.3

Approach to Cyber Defence

	Approach			
	Strategic	Tactical	Proactive	Reactive
P1	1	→	1	
P2	1	→	1	
P3		1	1	
P4	1	→	1	
P5	1	→	1	
P6		1		1
P7				
P8		1	1	
P9	1	→	1	
P10		1	1	
P11	1	→	1	
P12				
P13		1	1	
P14		1	1	
P15	1	→	1	
P16	1			1
P17		1		1
P18	1	→	1	
P19	1			1
P20				
P21				
P22				
P23	1	→	1	
P24				
P25	1	→	1	
P26	1			
P27				
P28				
P29	1	→	1	
P30	1	→	1	

> *The government should have the ability to regulate and/or fine companies for releasing products that may have detrimental effects on people's lives due to negligence or other. Software cannot be issued with a recall notice in the same way that a car can be recalled for faulty airbags. For example, some companies release poorly written software with privacy issues, and we've all seen what happens to easily compromised IoT devices.* – (P8)

Along with these recommended responsibilities, and in alignment with industry, participants commented that education and knowledge sharing should also be a

government responsibility. Participants believed governments should share the information they collect with industry so that organisations can make more informed decisions. Governments could also centralise protection as there are many agencies that hold citizens' information, and, with each controlling their own method of protection, standards of defence vary (Skatsson, 2020). Centralisation would also allow smaller agencies to use resources that, as individuals, they possibly could not afford (Skatsson, 2020). Centralisation and sharing information, potentially through the creation of more cooperative research centres, could speed up the discovery of new knowledge and the coverage of cyber defence, both of which would improve the security for Australia's information and infrastructure (Ministers for the Departments of Industry, Science, Energy and Resources, 2018).

Finally, and in a similar strategy to Israel's cybersecurity investments (Forrest, 2018; Frei, 2020), participants suggested that the Australian Government should provide more funding to those who operate in the cyber security sector:

> *I know that government can provide assistance to organisations should they require it under those circumstances. I think that the government, because they do fund universities, they need to ensure that they provide sufficient funding for universities to ramp up their capabilities for cybersecurity in general. I think it's got to the point where there should be funding specifically for cyber security.* - (P12)

5.4.2 Communication

The effectiveness of cyber defence also relies on the human element and the way individuals and groups apply technology and process. Therefore, in order to understand how effective organisational communication is, our research question asks, "Are Australian organisations and their employees aligned with regard to their perception of the threat of DDoS events?" Statistically, within the interviewed pool, most participants reported an alignment of threat perception (Table 5.4).

Table 5.4

Alignment of Threat Perceptions

Perceptions	Same	More	Less
Alignment	20	3	7

Twenty of the participants agreed that their level of risk was in line with that of their organisation and this view was generally derived from communications with their organisation. P25 stated:

> *I think we are on the same level. We have a lot of good communication so we're generally on the same page. The organisation has become more aware, so I think their assessment of the threat is perhaps more accurate. At least, I think they are more confident in their threat assessment now*.

P9 expressed a similar message:

> *I think we are about the same. As an organisation, our communication is pretty good, so I think we stay pretty consistent. The threat has grown in visibility, so I think the organisation's perception has grown as well*.

And P13 added:

> *I think we are on the same page with our thoughts about the DDoS threat. I'd also say it has increased, and I'd say this is due to the sophistication of cyber-attacks that has risen over the past decade*.

While the majority believe they and the organisation are in tune with their threat perception, many of the interviewees also added that the level of threat had increased over the recent time period. It is evident that for these groups, good internal organisational communication and equal access to knowledge and experience had brought alignment to their threat perception. The employees of the 10 organisations who mentioned that they were not aligned also highlighted communication in their comments:

> *At the moment [the organisation has] more, as they'll have a global view of attack vectors and probably more experience. My experience is from what I have seen and read, but the USA perhaps has greater exposure.* – (P24)

> *As the average Joe in a company, we live with a level of naivety compared to a practitioner or SMEs so they would be more aware of the reality of threats to an organisation than others in the field, even if they are in a technology area. It's such a highly specialised area and it sits under the veil of secrecy and confidentiality. [The organisation has] much higher levels of awareness of BCP (business continuity planning), risk and the need to be proactively securing business revenue from cybersecurity risks. In the last five years there has been a heightened awareness, not due to any one particular event,*

but due to a series of events around the world in the corporate and industrial areas. – (P29)

Both raise the probability that gaps in communication and lower access to knowledge lead to a misalignment of perception. A similar impression is gained from examining the comments from the seven participants who personally consider DDoS to be more of threat than their organisations do:

I believe they consider DDoS as less of threat. At least it has not been raised as a big issue to me. It [the threat] has increased, but this is due to the volume of phishing attempts we experience. [To help] they could train a network team to be able to work through a DDoS attack. Perhaps set up and run some training simulations. – (P20).

Phishing is a term that describes a cyber-attack where the instigator uses impersonation methods to gather sensitive information (Aleroud & Zhou, 2017). This is often in the form of forged emails or duplicated banking and payment sites. P20 and several others formed an opinion that the organisation's perceived level of threat is less than theirs as there is a lack of workplace discussion on the topic, lack of access to any risk analysis outcomes and lack of experience with the outcomes of cyber events. This difference of opinion can influence how cyber defence plans are conceived and implemented. If an employee's perception of threat is higher than that of the organisation, the justification for a project may be more difficult and approval may not be granted if value for expenditure cannot be seen. It is possible that organisation and employee can become aligned through discussion, as P7 states:

I think the organisation considers DDoS is less of a threat than I do, which obviously means if we do need to develop a mitigation plan or purchase any mitigation hardware/services, the organisation's consideration level may need to be revised. [The organisation's perception] has increased a little due to my constant discussions about cybersecurity. If we want to change the priority or focus, we going to need someone to champion the cause. – (P7)

Similarly, if the employee's perception of threat is lower than the organisation's, the employee may not be as vigilant and attentive in their approach to delivery and management of the mitigation solution. However, the opposite may also be true if the employee's perception is greater. They may take the initiative and champion the cause themselves.

As some groups are aligned while others are not, our research question asks, “Is this perception led more by individuals or by organisational culture?” Some level of reaction to the perceived responsibility is apparent, as shown in Table 5.5 as 23 of the 30 participants felt that the responsibility for driving learning and training sat with the organisation. This reliance on the organisation could mean that they expect to be led to the appropriate degree of threat.

Table 5.5

Education and Knowledge Responsibility

Responsible party	Yes
Organisation only	23
Individual only	2
Shared (organisation/individual)	4

However, six stated that they thought the responsibility should be carried by individuals (either themselves or others), and that it would be these individuals that should seek out knowledge and bring this understanding to the rest of the business. These six did, however, include four who believed that the responsibility should be shared across individuals and organisations.

Combining the results of alignment and responsibility, while 20 stated their perceptions were aligned, only four believed responsibility was shared. This may indicate that there is a high probability that employees follow organisational visions rather than being driven from within. The balance of power in organisations may be one reason why they feel compelled to follow leadership rather than risk the negative consequences of providing an alternative view. This information goes some way to answering the research question “Where should effort be focused to ensure Australian organisations are more prepared for a DDoS event?”, as employees believe organisations should be the driver. However, it is important to understand whether they believe organisations should act alone in this mission or if other groups share this responsibility. Therefore, to understand more deeply, a research question asks, “Where should effort be focused (by individuals, organisations, industry and government) to make the DDoS threat more widely understood by employees in Australian organisations?”

In this participant pool, IT teams made up approximately 2.04% of an organisation's total staff count when calculated as the mean average, or 3.76% with a median value, but individually, it was somewhere between 0.03% and 7.5% of total staff numbers. While IT teams are responsible for cybersecurity, many organisations have a primary purpose outside of that capability. Therefore, while cybersecurity may register as a priority for IT departments, it may be much less of a priority for the organisation as a whole. Organisations such as these would be more concerned that technology functions are maintained so that they can continue to operate their business. To them, cybersecurity is more of a component that enables their business to continue to operate efficiently. Therefore, it must fall to groups other than organisations and individual IT teams to drive cyber defence.

In the interviews, all participants stated what they thought the strategies of various groups should be but there were common themes within the wide variety of perspectives. One popular belief was that industry should take the lead in education and sharing knowledge. This knowledge transfer could be in the form of sharing information regarding recent attacks and mitigation outcomes (while keeping organisational anonymity), guidance on best practice and technology use cases and driving the creation of assessable industry training materials. Transparently sharing attack statistics, experiences and consequences could significantly assist other organisations to make more accurately informed choices regarding their own defence strategies and processes.

This study's website analysis found that little information was provided by organisations, and the literature analysis relied on information provided by organisations who own and manage cloud-based cyber mitigation services. Also, the study participants agreed that it is extremely difficult to gather detailed information on Australian cyber incidents, but this is something that participants felt would be of great benefit to the industry's community. In addition, participants felt that industry had a role to play in formal training capabilities. As P6 commented:

> *Industry is also best placed to direct education and training providers with the right coursework for staff to be effective in mitigating attacks.*

The collective industry understands the technology it creates as well as the threats it is subjected to and, consequently, through the outcomes of mitigation attempts, it

would also be best placed to provide advice on training requirements and course content. As participant P1 stated:

> *Industry should provide and improve mitigation technologies and techniques, but also educate and guide on best practices and use cases.*

The improved mitigation technologies and techniques mentioned place some focus on the technology created by industry. Many of the participants mentioned the need for industry to create more mitigation technologies but, as stated by P1, this comes with a caveat that while mitigation technologies and techniques should be improved, industry should also educate:

> *I'd say more education is required, particularly for SaaS product owners and developers (i.e., not just core IT). The organisation should be assessing the level of risk, weighing the consequences and building competencies to address those. Of course, industry has a role too. Industry should provide and improve mitigation technologies and techniques, but also educate and guide on best practices and use cases*.

Industry should also produce secure products that follow best practice and do not become a source used for attack. According to P8:

> *The industry needs to take more responsibility for putting out products that can't be compromised and included in a source for attack. When putting out products or services, they shouldn't ignore security best practices*

While industry should create safe and secure technology that is not vulnerable to attack and cannot be used in an attack, participants believed the governance of this should be the responsibility of government. Many participants called for legislation to mandate minimum levels of protection and methods for policing manufacturers' compliance. The government should also seek to protect Australian interests, which they could undertake in several ways. On a technical level, P18 suggests that:

> *The government, along with CERT Australia and ACSC (Australian Cyber Security Centre), could lead efforts to incapacitate the botnets used for DDoS attacks as well as publish IP blacklists so that known compromised internet addresses can be excluded from connectivity.*

On a governance level, governments could create guiding policy and seek to prosecute attackers from international jurisdictions. Using diplomacy, they should:

Champion industry and provide legal and diplomatic responses to nation tate attacks. – (P6)

5.4.3 Method

As shown in Table 5.6, the method of strategy or plan created varied considerably within the interviewed pool. Five indicated that their organisation had no plan and seven were unaware of the existence of any plan, with the latter, once again, highlighting the lack of transparency between organisational departments and employees. Of the remaining 17, over half (10) reported that their organisations ran their own in-house project, with nine of these using in-house expertise. The organisation of the remaining participant brought in an external expert to help with their project. Surprisingly, only six admitted that their organisation follows best practice guidance and frameworks such as NIST (Joint Task Force, 2018) or ISO27001 (ISO, 2021). As P18 stated:

> *We assessed the threats, outcomes and likelihoods in an organisational context and identified the 'key' threats for which response plans should exist. The plan development was then conducted following NIST Computer Incident Handling Guides (800-61 R2) to identify the 'detect, analyse, contain, eradicate and recover' steps. Resources (internal and external) were then identified to support the plans and made available as part of the preparedness work.*

Of those six, one had followed the outsourcing path (hence, little influence in the adherence to best practice) and a further three had procured the assistance of external expertise, which may suggest that external expertise is driving the adoption of best practice strategies. Also of interest is that only two mentioned the use of a risk assessment with a further three admitting to the development of BCPs.

Table 5.6

Method of Strategy of Plan Design

	Develop a BCP	**Out-source**	**In-house project**	**Internal expertise**	**External expertise**	**Followed best practice**	**Risk assessment**	**No plan**	**Don't know**
P1									1
P2	1								
P3		1							

	Develop a BCP	Out-source	In-house project	Internal expertise	External expertise	Followed best practice	Risk assessment	No plan	Don't know
P4			1		1				
P5	1								
P6					1	1			
P7								1	
P8			1	1					
P9			1	1					
P10					1	1			
P11							1		
P12								1	
P13			1	1					
P14									1
P15			1	1					
P16									1
P17								1	
P18			1	1	1	1			
P19		1				1			
P20									1
P21								1	
P22								1	
P23	1								
P24									1
P25			1	1					
P26			1	1		1			
P27									1
P28									1
P29			1	1		1			
P30			1	1			1		
Tot	**3**	**2**	**10**	**9**	**4**	**6**	**2**	**5**	**7**

This information helps to understand how organisations create their defensive strategies and plans and helps to answer the research question “How is the threat evaluated?” Logically, a risk assessment would be a commonly used step; however, in assessing the risk, the two respondents who revealed that their organisation had

performed a risk assessment said that it was this assessment that had revealed the threats that were addressed in their mitigation plan. Mentions of BCPs were also lower than expected. Why this was so is unclear, as the participant pool included employees from a wide range of roles, and it was therefore expected that terms such as these would be more commonly mentioned. It is possible that there is some misalignment between employer and employee, as one participant acknowledged that while this method was their preferred process, it was something that had not been undertaken by their organisation and there were no plans to do this in the future.

5.4.4 Motivation

Interviewees talked about how BCPs have helped their organisation to form their cyber-security strategies, but the motivation for creating these does not always come from the top down. While some organisations had put in place mitigations requested by their governance boards or their customer feedback, others relied on their own experience and internal intellectual property to determine their preferred defence approach. In some organisations, departments are granted authority to make strategic decisions, and with this, they are empowered to act swiftly to address emerging threats. As participant P2 said:

> *The business continuity plans are developed by the units to minimise the operational and financial impacts. I know that some involves deferring activity or in some cases using alternative infrastructure. We performed a threat and risk assessment for the organisation so some of these plans were uncovered during that work, but I expect other organisations would have something similar.*

While an organisation's own department may be the initiator, what motivates them to start? Several participants (six) noted risk as the motivator (As Table 5.7 shows, most participants' organisations follow a proactive approach; however, many participants mentioned the difficulty in obtaining a budget for a threat that may never eventuate:

> *Our challenges would come from the financial cost and, with that, getting the approval to spend a large sum on protection against an event that may never occur. It's easy to approve spends on backups as we see these in use*

frequently. It's a known and demonstrated risk. DDoS is more of an unknown. – (P7)

Table 5.7) with some using risk analysis to support their awareness. Others reported that their organisations did not assess the risk but instead simply followed recommended best practice, relying on the risk assessments distributed by governments, various vendors and/or adherence to popular standards such as NIST (Joint Task Force, 2018), the Australian Signals Directorate (ASD, 2020) and ISO (ISO, 2021). P29 explained their organisations reasoning:

> *A combination of two things. One is a growing general industry awareness of cybersecurity, risk exposure and then, as a consequence of that, business continuity threat, and in this case a DDoS attack would have impact on business revenue. So, an industry awareness and an internal awareness of keeping up with standards - Protecting the organisation's enterprise infrastructure and architecture.*

But, while the organisations did consider DDoS a risk, it was not considered significant enough to warrant single focus, and some organisations have chosen to group the threat of DDoS with their general cybersecurity strategy:

> *We are aware of the threats. We don't consider DDoS individually, but we consider it as part of our protection against other types of cyber-threats like hacking, theft and ransomware. We've made an assessment and we have planned accordingly.* – (P9)

As Table 5.7 shows, most participants' organisations follow a proactive approach; however, many participants mentioned the difficulty in obtaining a budget for a threat that may never eventuate:

> *Our challenges would come from the financial cost and, with that, getting the approval to spend a large sum on protection against an event that may never occur. It's easy to approve spends on backups as we see these in use frequently. It's a known and demonstrated risk. DDoS is more of an unknown.* – (P7)

Table 5.7

DDoS Defence Motivation with Victim/Reactive Relationship

	Approach		**Motivation**				
	Pro-active	Re-active	Results of Risk Assessment	Standard Practice	Customer Expectations	Victim	Legal/ Regulatory
P1	1						
P2	1		1				
P3	1			1			
P4	1				1		
P5	1			1			
P6		1	←	←	←	1	
P7			1				
P8	1				1		
P9	1			1			
P10	1				1		
P11	1		1				
P12							
P13	1				1		

	Approach			Motivation		
P14	1			1		
P15	1			1		
P16		1			1	
P17		1			1	
P18	1		1			1
P19		1			1	
P20						
P21						
P22				1		
P23	1		1			
P24				1		
P25	1			1		
P26				1		
P27						
P28				1		
P29	1			1		
P30	1		1			

> *In previous experiences with implementing a DDoS mitigation plan, the debate raged around value verses expenditure for such a service. For example, what if we pay for it and never experience a DDoS verse? What if we don't pay for it and we do? And what happens if we pay for a service and experience a DDoS anyway, is there any point as, can our network handle the prevention of an attack? One of the biggest challenges for implementing such a plan is making sure we cover the most common vectors of attack and making sure that either the blocking or scrubbing device or scrubbing service can handle the load.* – (P4)

> *Understanding the size of the threat and convincing the decision makers that there is value in defending. The value may only be realised if an attack eventuates so until that happens, it's hard sometimes to understand the reason for the investment.* – (P9)

Those organisations that were reported by the participants to have previously been a victim (n=6) formed reactively implemented defences, but the participants revealed that budget approval was much simpler when supported by first-hand experience:

> *Historically, the key challenge was investment. Knowing that we're under attack constantly/daily and not having any incidents arising from that is a good thing but when you're looking for investment, nothing bad happens (and*

so what's the problem?). People say "Yes, you're doing a fantastic job but we're not going to give you more money because you're doing a fantastic job". That's the key challenge and I suspect that's a key challenge for a lot of people. – (P19)

Spending budget on a defence technology that has a low chance of being used is a big challenge. We might spend a few hundred thousand on a mitigation service and never get an attack. If that happened it might be seen as a poor investment but if it defended an attack, it would be value for money. We can quantify the consequence, the hard part would by quantifying the risk. – (P30)

5.4.5 Risk Ownership

Risk transference is one of the common strategies in risk management (the others being accept, avoid, reduce, and share) (Joint Task Force, 2018). Ensuring that another agency takes on all or part of the risk serves to lower the risk level for the organisation. In cybersecurity, risk transference can occur in several ways. It is possible to insure against the losses caused by cybersecurity incidents as one would insure a house or car against accident, fire or theft (Franklin et al., 2009). An organisation can also rely on an external company for cybersecurity, or have it included as part of a cloud service contract, where there is an agreed level of defence incorporated into service agreement:

We outsource IT matters to a third party, so I presume they have policies in place to deal with it but am not sure. When we set up the firm four years ago, they were recommended by a client as a company that could handle our IT needs. They have done a good job to date, so we keep using them. – (P3)

In this participant's case they outsourced control of their IT systems to a third party effectively transferring the risk through a contractual obligation. Another form of risk transference appears in the form of insurance. Insuring against the risk of a cyber-attack will not reduce the likelihood, but may help with the various costs associated with it, such as liability (including privacy lawsuits and legal defence), financial loss, and the costs associated with the response itself, such as over time, and external expertise:

We have cyber insurance and clearly the people that run the cyber insurance, and in fact the insurance function itself, are also members of the critical

incident management group, but way down the bottom because, quite honestly, they are there to observe and collate information for a later claim. They are post event action. – (P1)

Another form of risk transfer was also raised. One participant stated that they "had a team that looks after security". This is an internal transfer of risk as the risk still sits within the organisation, but responsibility is placed more specifically on a single department.

Risk transfer is an effective way to reduce risk, but consequence is a separate consideration. Risks are rated on a combination of likelihood and consequence. When a risk eventuates, negative consequences can still affect the organisation even if contractual obligations push the onus of accountability onto a third party. For example, if, as a result of a DDoS attack, a company could no longer deliver orders to customers, the company could still incur a reputational loss even though the responsibility for cyber defence (supported by contractual threat of financial penalty clauses) may have been transferred to a service provider.

5.4.6 Risk

To support the research question "How high do Australian organisations rate DDoS as a threat, when compared to other cyber security events?", there are many risks (several noted in

Table 5.10

) and, while only one of the participants rated DDoS as their highest threat, this does not mean it has been discounted by others. 84% of respondents agreed that DDoS was a valid threat. While most did not identify it as their organisation's greatest threat, over half declared it a sufficient enough threat to have provisions for DDoS mitigation included in their organisation's cyber defence plans, and 57% of participants believed the threat of a DDoS attack was sufficient enough to drive the creation of a mitigation plan.

However, reputational damage and an inability to operate are still costly exercises and require that organisations plan for such events. It is common practice to produce a risk register that details the known or expected risks associated with strategic plans and operational activities. Risk registers comprise likelihood (as a measured likelihood of

occurrence) and consequences (as a measure of the scale of loss), and together these measurements help to calculate a risk's priority. Following the establishment of a risk register, plans are generally created to mitigate these acknowledged risks. In this study, 57% of the respondents advised that their company had contingency plans to mitigate future DDoS attacks, four said they were not able to comment on the existence of plans and 30% (n=9) stated that a plan did not exist, despite the overall majority agreeing it was a valid threat (Table 5.8).

Table 5.8

Organisations with Cyber Security Plans

Plan (in place or in development)	Occurrence
Yes	17
No	9
Unsure/Don't Know	4

Around five chose 'accept' as their organisation's mitigation strategy, with some commenting that they believed their organisation was not a likely target (Table 5.9).

Table 5.9

Risk Mitigation Method

Risk mitigation method	Occurrence
Avoid	0
Reduce	17
Transfer	8
Accept	5

Accepting a risk is usually restricted to those risks where the potential consequences are low enough that the consequences of their occurrence can be tolerated. For example, the use of the internet present risks but many businesses would be unable to function as efficiently without it, which may explain why no one chose the 'avoid' strategy. The 'avoid' strategy seeks to eliminate all possible risks by abstaining from actions that create a risk opportunity, but as technology and connectivity are so intertwined in everyday businesses, most organisations would suffer if they heavily restricted or removed internet functionality from their processes. The five that chose the 'accept' mitigation method found that the risks were sufficiently low for there to be no benefit from investment in defence. For example, with minimal exposure, P22 was concerned with what to them was a greater threat:

We consider data breach, phishing and crypto/ransomware to be more of a risk than DDoS. Our external facing entity is a static web page and it is hosted with a third-party hosting provider, so it's away from our perimeter completely.

As Table 5.9 shows, the majority of the organisations have chosen to reduce their risk. They use a variety of methods that are not limited to technical solutions such as software and hardware. Some put in place plans to switch to alternate processes such as manual processing should a DDoS attack affect their system's capability and capacity, with one participant stating:

In my organisation, we could fall back to manual processes where possible. The idea would be to get away from digital as quickly as possible. – (P23)

Another identified the difference between cloud infrastructure and the organisation's own local network, suggesting that if their own network was compromised, their service on cloud infrastructure would still be able to service their customers:

The main part of the plan is to reduce reliance on the network. Given that a DDoS attack would be to specifically bring down said network, what controls do we have and what alternates do we have to continue to provide services? And that's where the focus has been. So, we have a lot of cloud services where we basically hold our providers to ISO 27000 series control. So, we have access to those and if not, we have alternatives. – (P19)

As expected, many organisations had adopted technical solutions that utilised hardware devices that are backed up with processes that formalise stakeholder communication:

The organisation has formal contingency plans to mitigate DDOS attacks – including a dedicated computer security team, hardware-based security devices including VPN, firewalls, load balancing, and an established escalation process where all staff have agency to notify stakeholders of an emerging threat. – (P6)

Also, in many cases, organisations have established monitoring to provide alerts of attacks, with one participant mentioning that they had implemented methods to prevent their own potential utilisation for future attacks:

> *We have monitoring in place, and we reactively deal with DDoS. Some filtering of protocols and hardening of our equipment goes a long way to making sure we are not participants in DDOS attacks as well.* – (P14)

Another participant mentioned that:

> *We have several contingency plans. We've implemented extensive fine-grained monitoring. We've a 24x7 operation centre in place and have DDoS blackholing service capability. We're also looking at DDoS Scrubbing and this should be coming soon.* – (P11)

Eight of the participants indicated that their organisations have chosen to transfer risk. This is a significant number (26%) and a mitigation strategy that should be observed more closely. Over time, this percentage may rise as more organisations choose to move their systems to cloud hosting providers, but this is not a certainty as many large businesses have chosen to retain control of selected areas of their environment. It is possible that cybersecurity could be one of the areas chosen to remain under organisational control – a view supported by the Australian Cyber Security Centre (ACSC), which recommends "seriously considering the potential risks involved in handing over control of organisational data to an external vendor" and that the use of offshore vendors may increase that risk (ASD, 2020, para 4). P30 worked for one such organisation who went against that advice:

> *We don't have anything specifically for DDoS. It's part of our overall strategy that we are still yet to find time to tackle that issue. Some time ago, we moved several of our systems to the cloud. It's a gradual process but those that are there, benefit from the supplier's defence capabilities that are a defence for us. Our remaining on premise systems don't have that.* – (P30)

Overall, the perceived level of risk reported by the participants varied from one who thought there was no real threat to very high, such as those who specifically commented that it was a real threat to their organisation. As shown in Table 5.9, no organisation has chosen to avoid the threat and only five participants indicated that their organisation has chosen to accept it, which suggests that the threat is known to these organisations but considered unlikely or easily accommodated with little effort. The remaining majority of the participants (n=25) reported that their organisations have chosen mitigation methods that require contentious effort to plan and

communicate, which suggests that the level of threat is considered large enough to justify these actions.

Consequence is the second attribute of risk analysis. While risk (or level of threat) is concerned with the probability of an event occurring, consequence reflects the scale of the impact once the event has occurred. For consequence perceptions, several comments help with understanding:

> *Understanding the size of the threat and convincing the decision makers that there is value in defending. The value may only be realised if an attack eventuates, so until that happens, it's hard sometimes to understand the reason for the investment.* – (P9)

> *The challenges are getting people across to the belief it is a real threat. If it hasn't happened, it's harder to convince people and they need to understand the threat is real before we could get any traction.* – (P24)

These comments refer to the problem of justifying budget requests to fund mitigation plans. Without evidence or experience of the consequence of a DDoS attack, funding arguments can be difficult to defend. Little if any information regarding the result of DDoS attacks is made publicly available by victim organisations, such that only those organisations that have previously been victims themselves have the capability to accurately assess the consequence of a potential DDoS attack.

This lack of information may be why cybersecurity leaders group the threats to present proposals for cyber defence projects and associated funding. As another participant commented:

> *The justification for a specific attack vector may be a more difficult argument than proposing an overall defence plan. So, if we're arguing for DDoS specifically, we'd probably get more traction if it was part of a plan.* (P15)

Therefore, along with the level of threat, consequences are considered within a full range. Those businesses that have little reliance on technology and minimal experience with DDoS attacks find the consequence to be low; however, those businesses that have experienced an attack assess the consequence as 'high enough' to not want to experience it again.

5.4.7 Threat

During the interviews, participants first discussed the credibility of a DDoS threat, and of the 30 participants, five considered the threat to be non-valid. That is to say, around 17% did not consider DDoS to be a credible threat to their organisation at all. Table 5.10 shows that participants believed that data loss/theft and the loss of PII and PCI could be a more impactful risk. However, several participants commented on the potential for reputational damage to occur if this type of secured information were to be exposed, which could be comparatively more damaging to the organisation. For example, one respondent said:

> *The loss of data would impact us directly but also the reputation risk if we were to lose data we hold for others. Reputational risk can be more damaging as the effects could last for a long time.* (P9)

Table 5.10

Primary Cyber Security Risk/Threat

Type of risk/threat	**Frequency of response**	
	Threat	Risk
Vandalism		2
State terrorism event	1	
Social engineering	7	
Ransomware	6	
PII-PCI-PHI		9
Phishing	6	
Non-cyber threat		
Malware	2	
Loss of intellectual property		5
Insider attack e.g., rogue admin	2	
Infrastructure compromised		2
Human error	6	
DDoS	1	
Data loss, theft		16
Reputational loss		8

The highest threats were observed to be those that encounter human interaction, such as social engineering, ransomware and phishing, all of which require human input to be successful. Others highlighted the potential impact of human error, whether that is through human error or coercement via social engineering, with responses such as:

> *I think unauthorised access to the environment whether it's via social engineering or another method would be a greater threat. Someone gaining access could lead to loss of IP [intellectual property], loss of data or we could suffer vandalism.* – (P7)
>
> *People can make mistakes, so we try to develop processes that reduce the chance of errors, but anything that succeeds in stealing that information could cause us some problems.* – (P30)

However, even when the majority seemed to be most fearful of data loss and exposure, their major concern was that the consequence of any attack may lead to an enduring loss of reputation for their organisation that brings on an inability to operate, as opposed to a specific event that directly ceases operations or exposes intellectual property. Reputational damage from exposed personal information may last for some time and a DDoS attack could have a similar result. Agrafiotis et al. (2018) suggest that reputational damage may comprise several outcomes: damaged public perception, reduced corporate goodwill and damaged relationship with customers and suppliers. For example, a DDoS attack that prevented bank account holders from accessing their funds may cause a significant amount of customer distrust. Inability to recruit staff or loss of existing staff (including loss of knowledge and intellectual property) may be other forms of organisational harm that may prove to be longer lasting (Agrafiotis et al., 2018).

How long these reputational impacts last has not been well studied, but the literature suggests that the impact could be costly but publicly short lived if customer communication is performed well. For instance, using situational crisis communication theory (SCCT) guidelines, the organisation could aim to match its effort and expenditure on resolutions with customer expectations and ultimately improve their crisis response strategies (Coombs, 2007). However, in addition to the publicly observed impacts, organisations can suffer longer-term difficulties as they navigate through incident triage, impact management and the months or years they commit to business recovery (Mossburg et al., 2016). This may go some way to explain why most websites do not mention details of recent and more distant cyber events.

5.5 Demographics

According to ABS data, in 2020, Australia had approximately 2.4 million businesses with around 60,000 of these being classified as medium and large scale and a further 930,000 classified as small (ABS, 2020a). The ABS categorises businesses with 5–19 staff as small businesses, 20–199 staff as medium business and over 200 staff as large organisations (ABS, 2010). The 'small' classification also includes a subgroup of 1–4 employees named micro, which constitutes the majority (711,000) of businesses in this subclass (ABS, 2020a). A smaller classification also exists for ABN registered businesses with zero employees and that are not GST registered. The classification name for these business types is nano business (ASBFEO, 2017); however, no micro or nano businesses were identified as potential participants for this study. Most of the medium and large organisations could be expected to have a designated and specific department that tackles IT and cybersecurity-related workloads (Whitman & Mattord, 2017). The results of this study agree, with all but one of the respondents stating that their organisation does have a specific IT department. The one exception stated the reason for this is because the organisation "outsources IT matters to a third party" - (P3).

All the study participants selected were from Australian medium and large-sized businesses (ABS, 2010). Of a total of 110 participants approached, only two declined to participate in the interviews, 67 did not reply to the invitation and 41 agreed to interview; however, 11 of these either changed their mind or ceased contact following their agreement to be interviewed. Figure 5.8 shows the proportions of these groups:

- 'Complete' indicates the number of participants that were approached and an interview completed.
- 'No' indicates the number of individuals that were approached but rejected the offer.
- 'No Reply' indicates the number of individuals that were approached but did not respond to the initial request or subsequent follow-up communications.
- 'Ghosted' indicates the number of individuals who were approached and accepted the invitation to attend but then did not respond to any further follow-up communication (Green, 2019; Hamann, 2019; Wigmore, 2019).

A further 11 individuals were identified but they were considered ineligible as their organisation's employee count was too small for the limits set for the study (Medium and Large Organisations in Australia (ABS, 2010)). Businesses excluded were those with fewer than 19 staff.

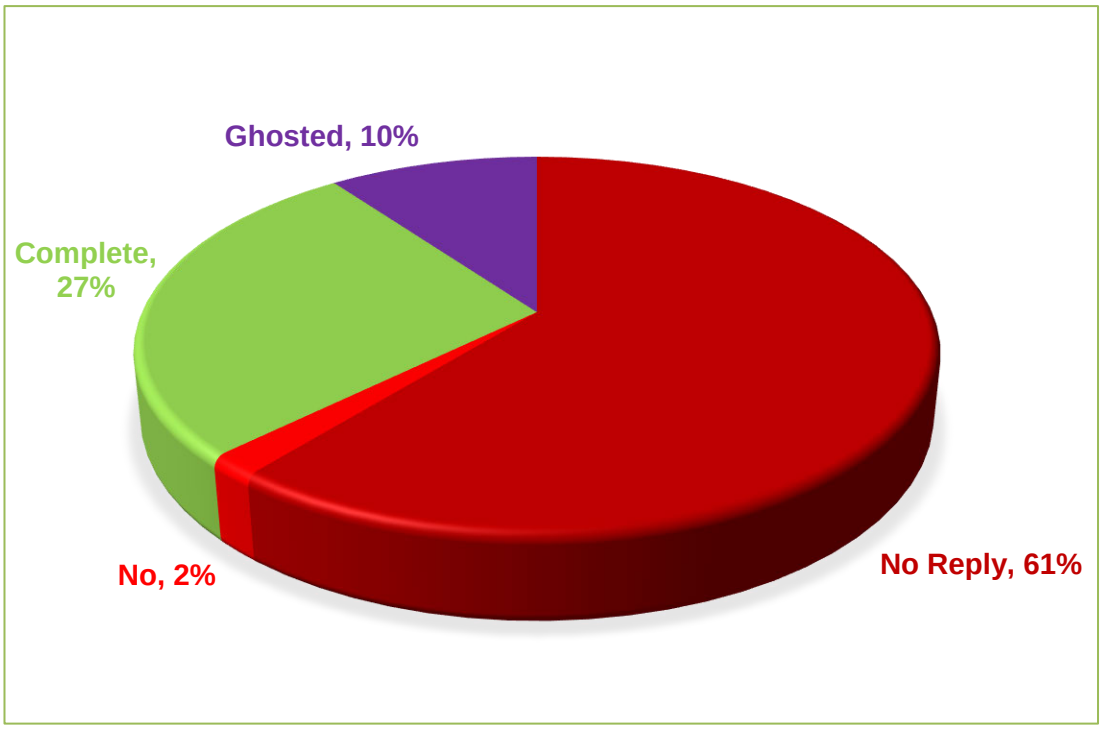


Figure 5.8. Response statistics

The websites that were analysed contained a mix of the organisations that were interviewed and the organisations where interviews did not occur. The websites analysed represented a broad base of sectors as classified by the ABS (2020a). Three sectors provided most of the websites analysed: information media and telecommunications, professional, scientific and technical services and education and training'. The least areas analysed were mining, healthcare and wholesale trade (Figure 5.9).

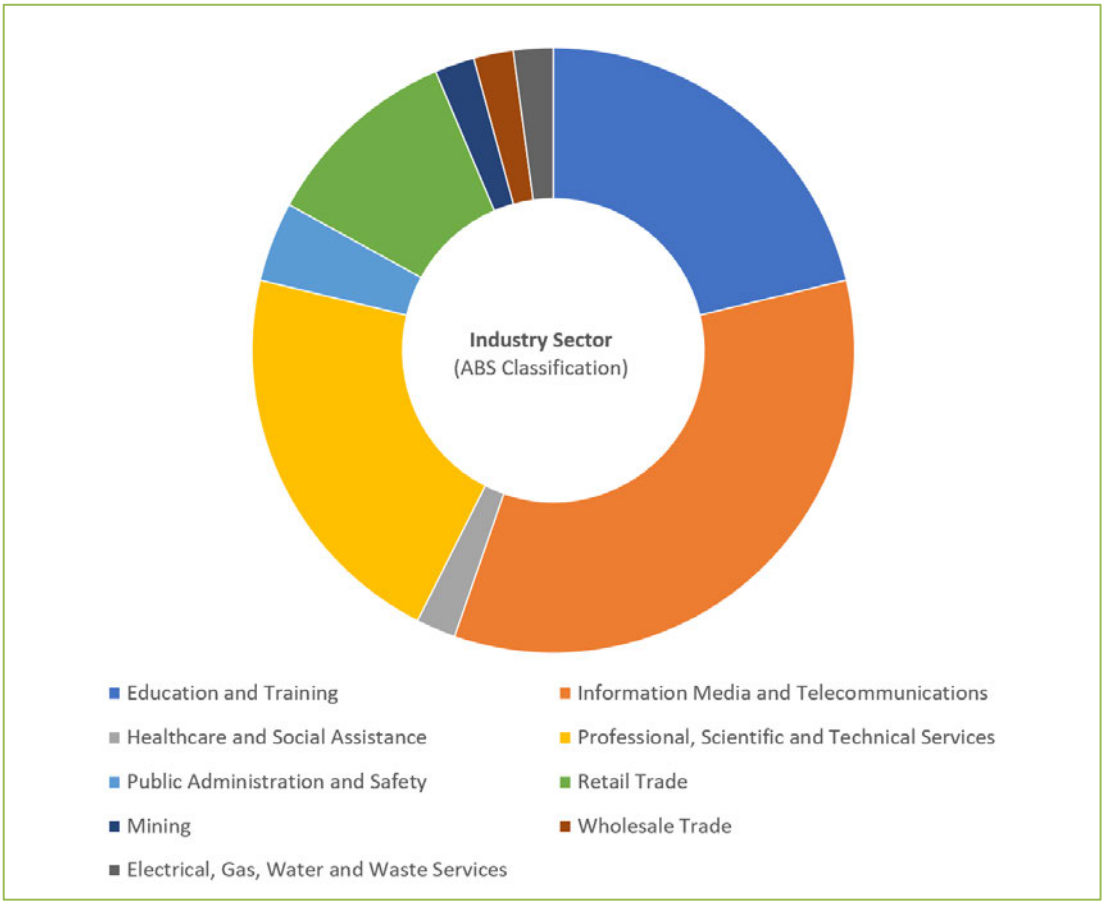


Figure 5.9. Analysed websites by ABS sector classification

The proportions of businesses in the sectors included in the analysed websites group did not match the overall proportions seen across Australian sectors (Figure 5.10), with information media forming a greater proportion within the interviewed range in this study, as shown in Figure 5.9.

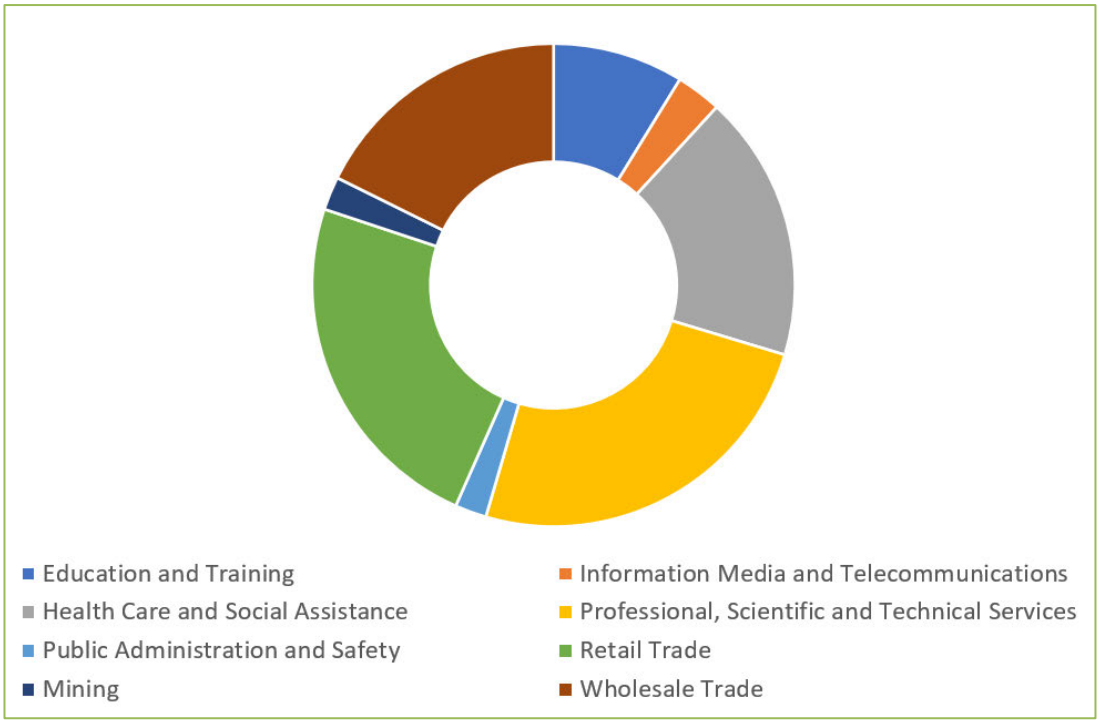


Figure 5.10. Total medium and large businesses in Australia by ABS sector classification (ABS, 2020a).

The ABS categorises organisations into 18 primary sectors. This study examined just under 50% of these; however, as shown in Figure 5.11, requests were sent to 12 of the 18 sectors.

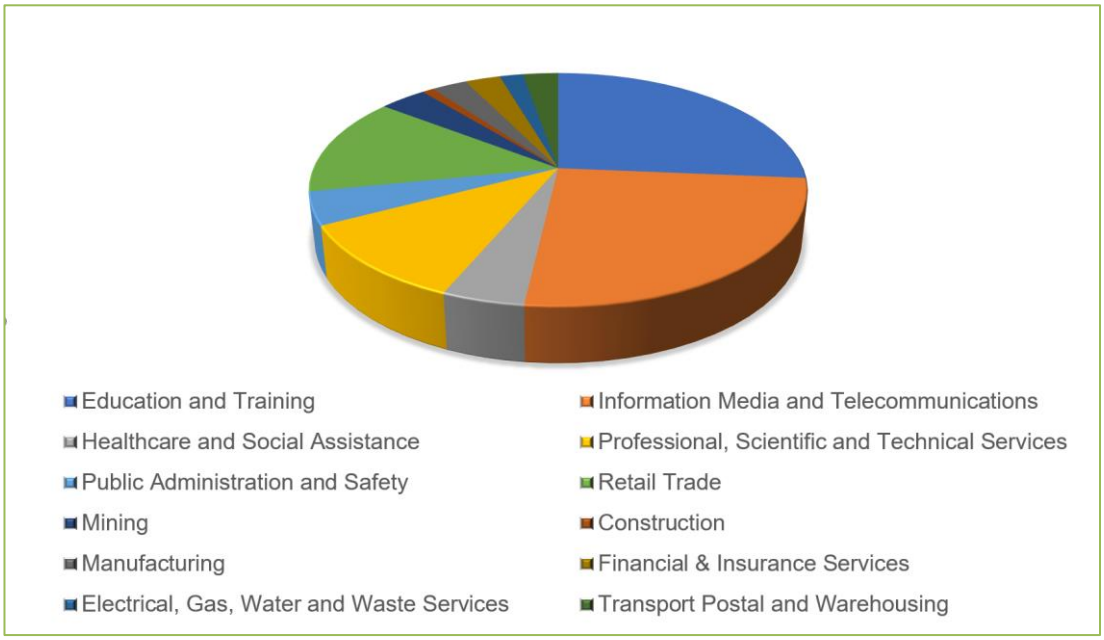


Figure 5.11. Participant by sector representation

As shown in Figure 5.12, medium-sized organisations in this study are not well represented in the manufacturing, mining, healthcare, wholesale-trade and utilities sectors. This may be due to the limited numbers of medium-sized businesses that operate in these sectors, as they are businesses that generally operate in larger national and international markets.

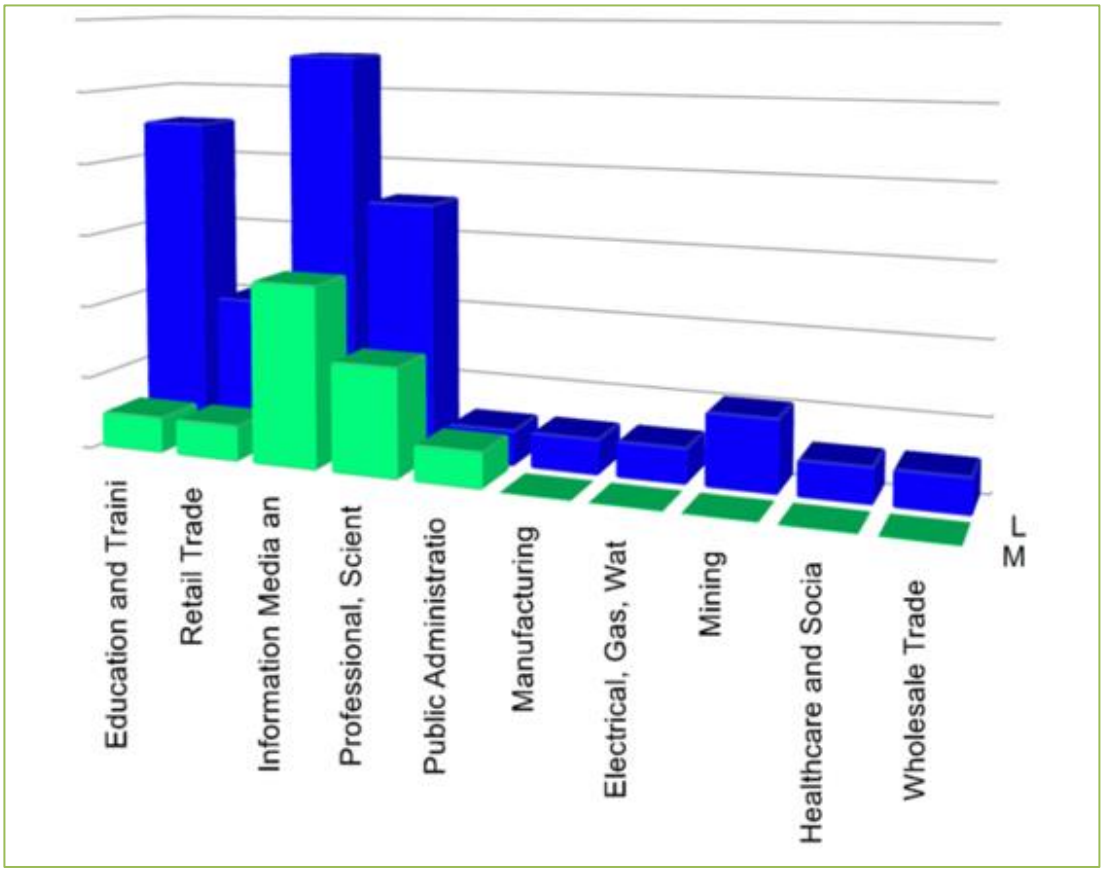


Figure 5.12. Medium and large organisations per sector

Very few invitees from the public administration, healthcare and mining sectors agreed to be interviewed (Figure 5.13), despite all approached organisations having dedicated IT and security departments with staff who would very likely be suitably qualified participants.

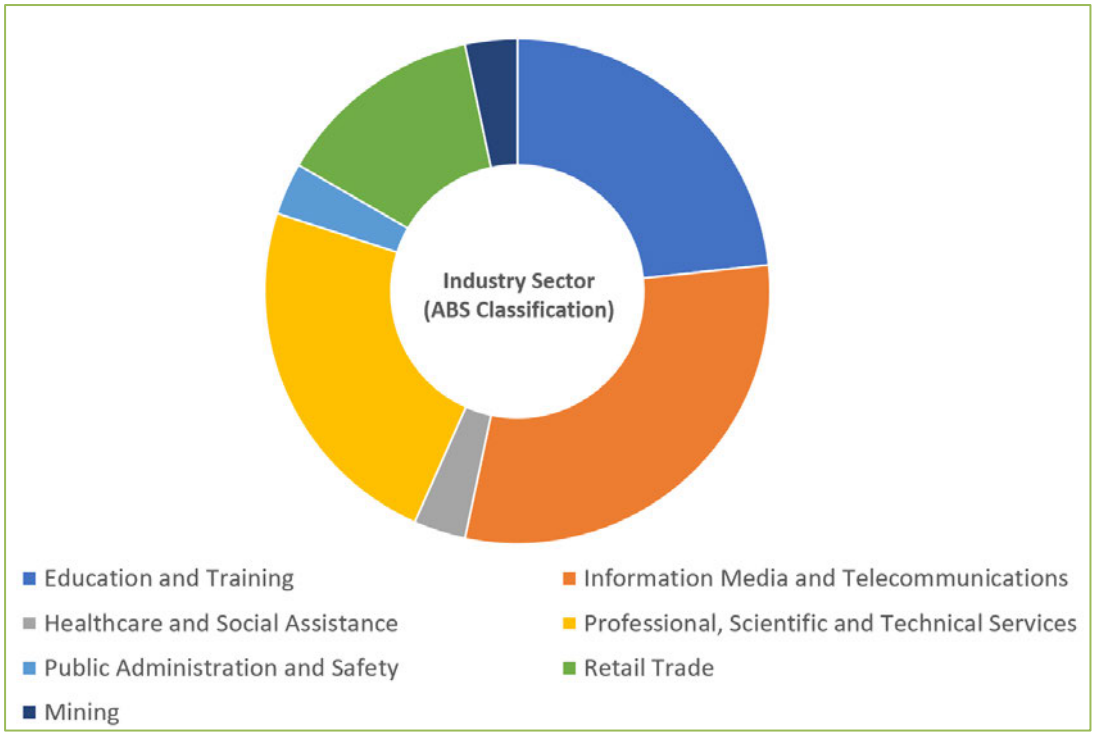


Figure 5.13. Interviewed respondents by ABS sector classification

This failure to obtain a response remains unexplained due to the lack of communication but may include potential reasons such as organisational policy that prevents information release, fear of exposure or conflicting workload. These reasons are discussed in more depth in Chapter 6.

The ABS has eight classifications for roles identified by skill level: managers, professionals, technicians and trade workers, clerical and administrative workers, sales workers, machinery operators and drivers, and labourers (ABS, 2020b). As highlighted in Figure 5.14, in medium and large Australian organisations, male employees hold the majority (over 80%) of roles classified as technicians and trades whereas there is a more even distribution for managers and professionals (ABS, 2020b). Rosenbloom et al. (2008) suggest that this is due to the differing interests of men and women, which may be due to the differing levels of interest shown during the high school years (Sadler et al., 2012). Little (2020) discusses the lack of gender equality in technology firms and the high number of female employees who leave before completing one year's tenure. Sadler et al. (2012) had similar findings, and suggest this situation may be due to female lack of interest in high school being possibly attributed to lack of female role models in these careers.

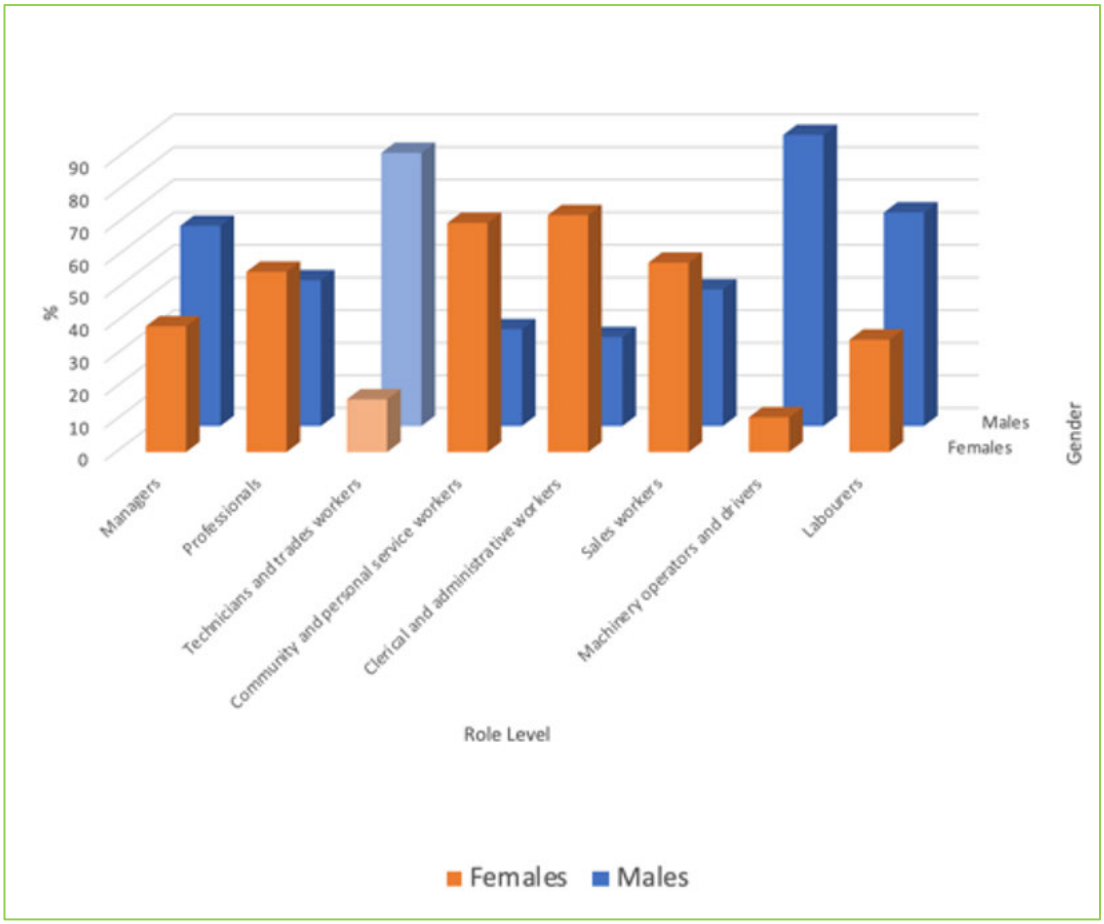


Figure 5.14. Occupation by gender 2019–2020 (from ABS (2020b))

As a percentage of the overall invitations to participate that were sent, the demographic results show that more males were approached (Figure 5.15). However, of those approached, more females agreed to participate (Figure 5.15). These results may align with the findings of Kolenko (2019), who found that the more nurturing characteristics displayed by feminine cultures feeds an interest in protecting others. This unequal division of participants does not align with the sector by gender figures from the ABS (2018) or the overall gender workforce figures from 2019–2020, which showed 67.6% of females and 78.1% of males participated in the workforce (ABS, 2020b).

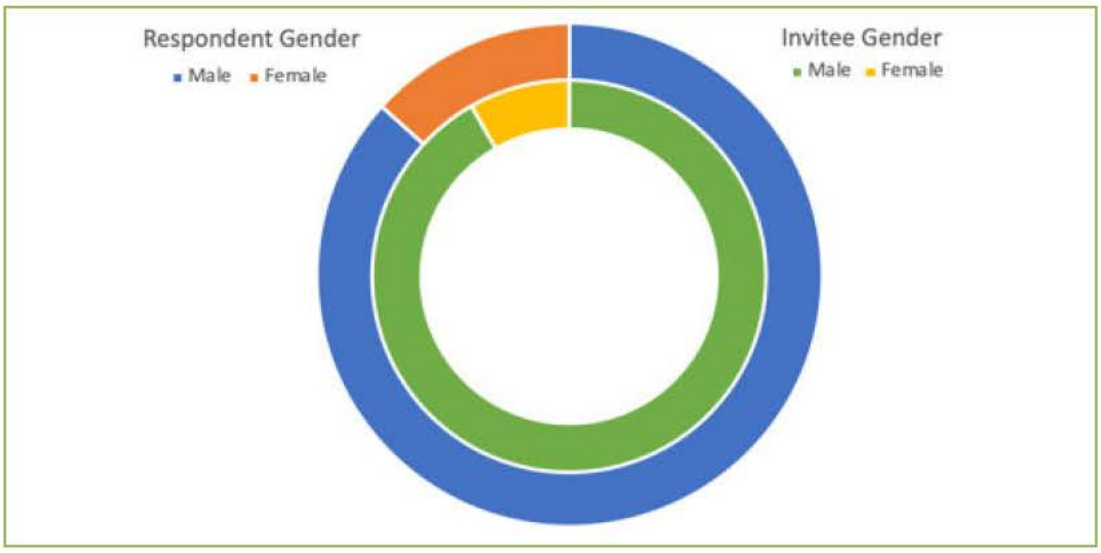


Figure 5.15. Invitee vs respondent (gender)

In the pool of participants, there were proportionately more females in technical roles than either management or leadership. Of the respondents who agreed to participate, approximately 15% of technical roles, 10% of manager roles and 33% of leader roles were held by females (Figure 5.16).

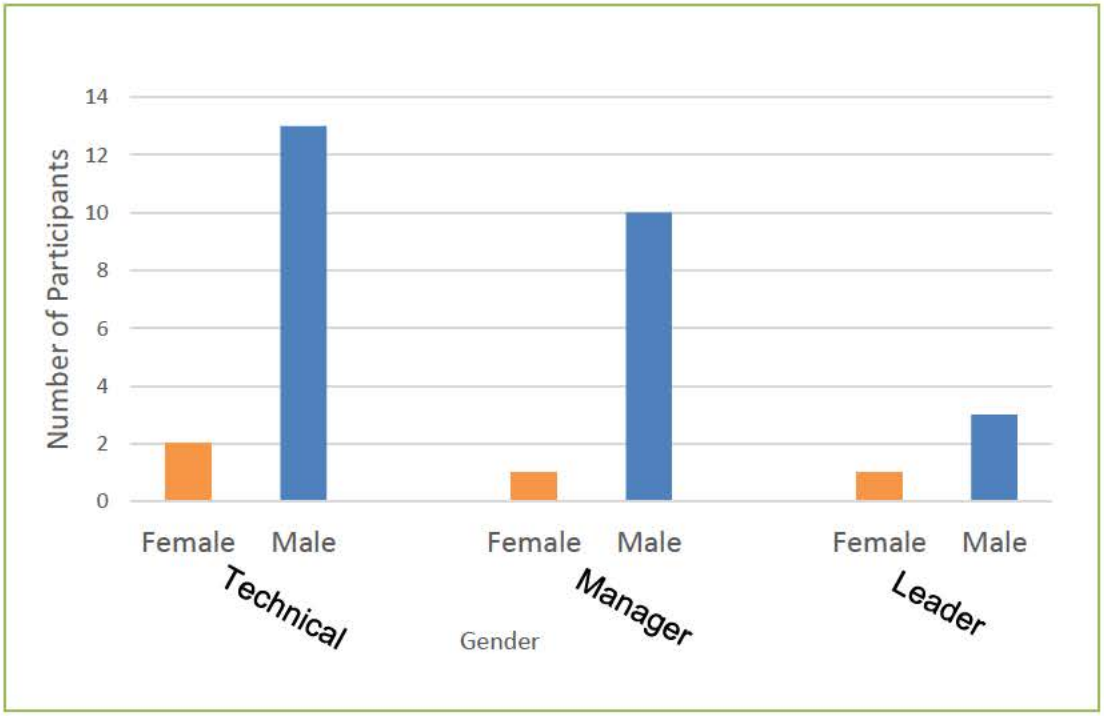


Figure 5.16. Role and gender

As shown in Figure 5.17, the tenure of leaders and managers with a single organisation was predominantly less than five years, with only one of the participants continuing

employment beyond that. One reason for this is that a leader may reach a stage where they become dysfunctional (Shapira, 2019). Aghion and Jackson (2016) suggest that over time, leaders become less willing to take risky actions through fear of exposing their level of competence or incompetence, and it is this lack of action that ultimately leads to their removal. However, this removal requires their superior to have higher motivated expectations; however, if a superior has also reached a dysfunctional stage, decision risk levels may fall, leading to longer terms of tenure despite lower levels of delivery. Those in technical roles had a tenure spread evenly across all the duration categories. While traditional career paths saw management promotions offered to those who excelled in technical roles, by the 2020s, other work–life rewards were considered equally attractive, and these technical staff can often find ways to acquire job satisfaction (such as salary, life balance, fame) without moving away from the roles that fulfil their passion (Madhra, 2017).

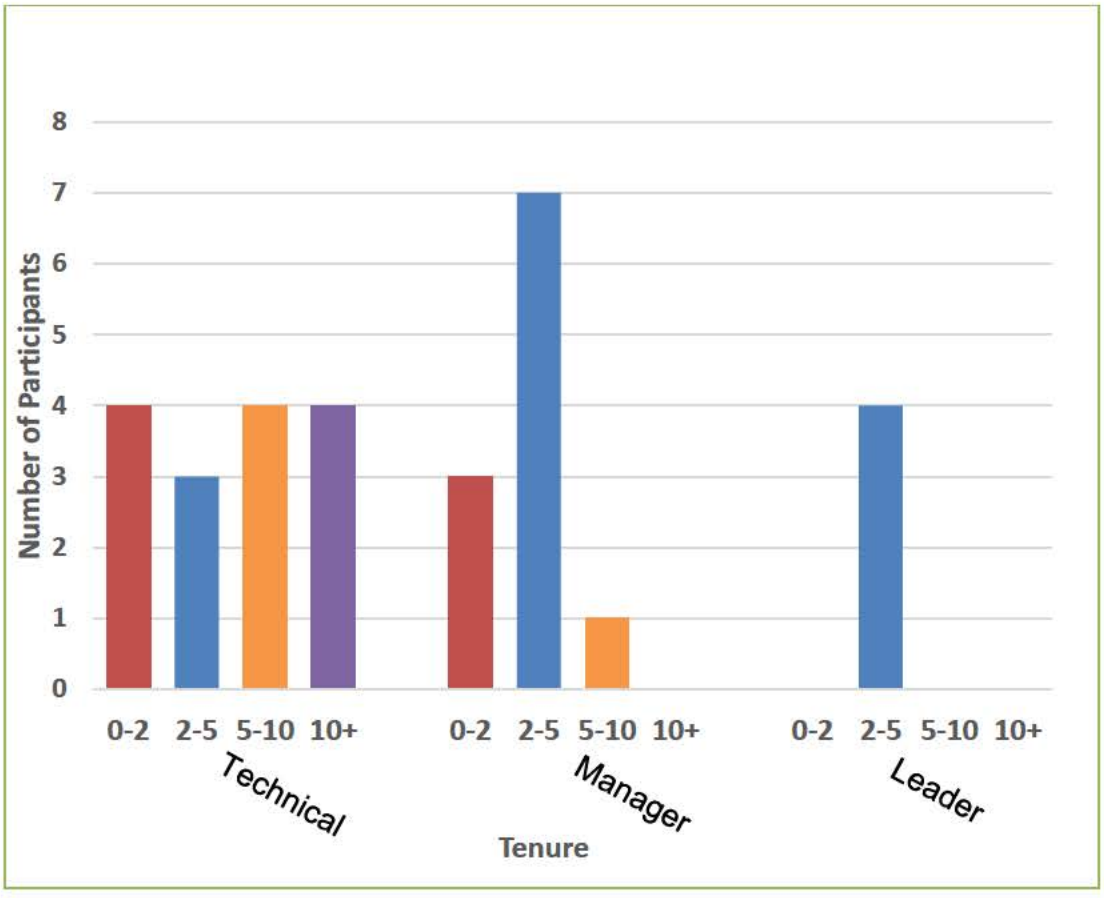


Figure 5.17. Participants' role and tenure

IT team size across the participant group was predominantly at 10 or below, with larger team sizes occurring less frequently. Very few organisations had teams of over 25 staff (Figure 5.18), despite the largest organisational staff numbers being in the range of 250 to 80,000. Only two participants had teams larger than 100 staff.

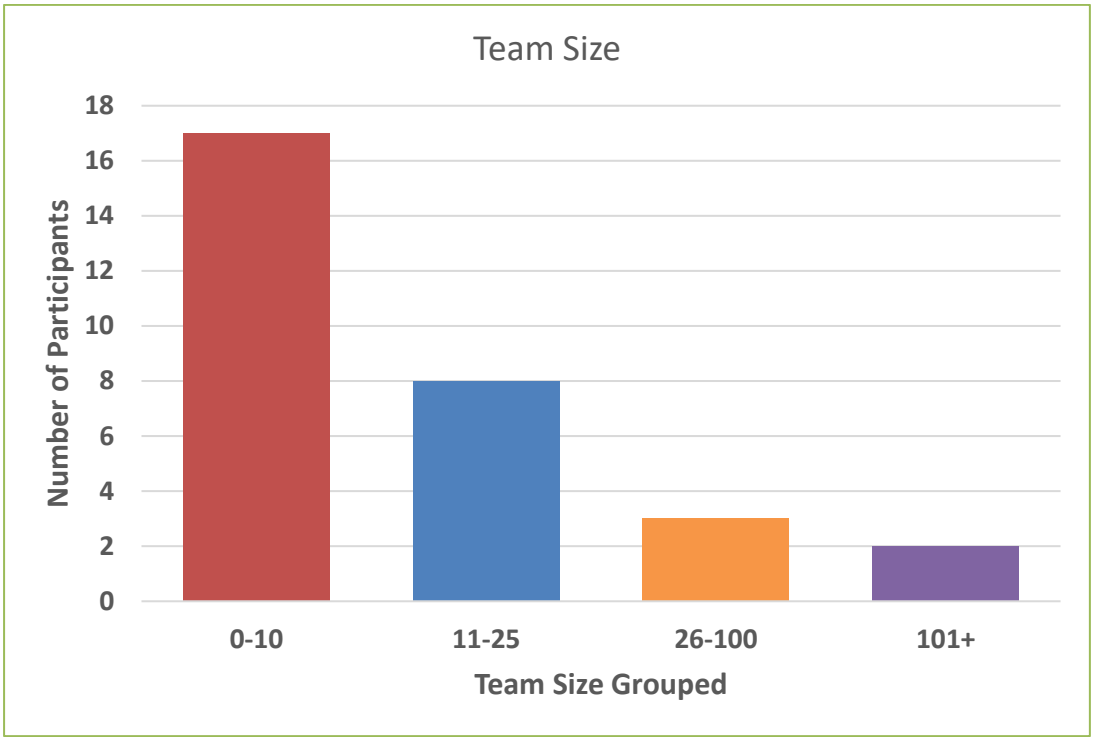


Figure 5.18. Team size

Larger team sizes were in organisations that had a national presence; however, one Victorian-based organisation did have a team with over 101 members (Figure 5.19). For categorisation, national businesses were considered to be those that had a presence in multiple states in contrast to those that had a formal location in only one state but also may supply products and services nationally. Even though an organisation with a multiple location design has centralisation of core services, there is often an additional overhead for technology teams as each location requires a level of individual attention, which means technology team sizes must increase to provide sufficient capability.

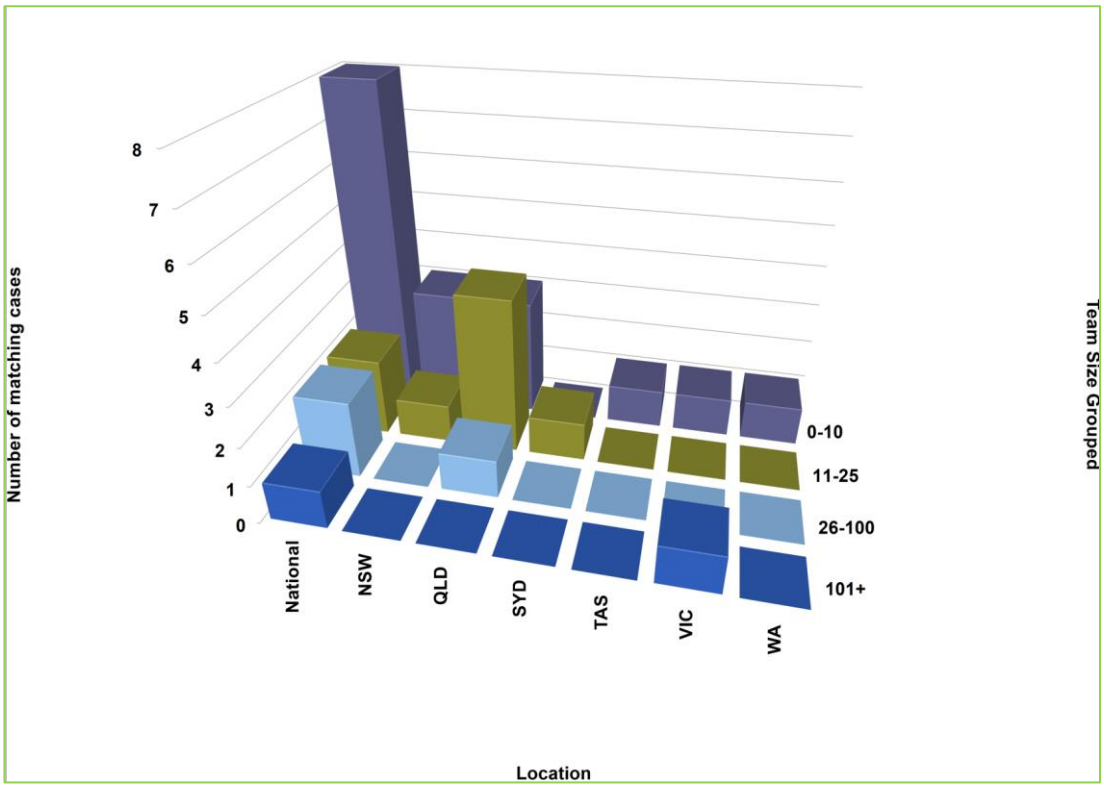


Figure 5.19. Team size and location

Of the organisations interviewed, only seven of the participants offered confirmation that their organisation had been a victim of a DDoS attack. In these cases, all victims were confirmed to be large national and regional organisations.

5.6 Summary

This chapter began with a description of the major themes found during an extensive literature review that covered both academic and practitioner sources. These literature reviews showed the consolidated themes of approach, communication, method, motivation, risk ownership, risk and threat, but also revealed initial areas where gaps in knowledge existed. The results of the website analysis allowed deeper investigation of the macro themes, which brought greater understanding of the topic. The study found that over half of the websites analysed had no cybersecurity information, which was in contrast to the privacy and trading terms information that as a legal requirement were much more visible. Cybersecurity information is published on a voluntary basis, and this lack of information aligns with organisations' reluctance to share and collaborate in this area. Assessing the content of what was published showed that those

who agreed to be interviewed shared marginally more information online than those who declined, and analysis of language complexity showed that those who did not share cybersecurity information used language that was appropriate for a younger reading age group. Also, while most organisations resisted sharing information, it seems they were equally resistant to the receipt of information, as 66% of websites had no way to report or inquire about cybersecurity incidents. This analysis provided direction for the semi-structured interviews that followed. The lack of willingness to share cybersecurity information was seen in the interview participant acceptance rate of 27%; however, within the seven macro themes identified in the literature review and investigated through website analysis, new knowledge was generated for six of these through the interview program. These new findings and deeper analysis of the results are discussed in the next chapter (Chapter 6 – Discussion).

Chapter 6: Discussion

6.1 Introduction

In the previous chapter, the results of the literature review, website analysis and interviews were collated, assessed and presented. In that chapter, the existing literature was used to build a base of understanding from which to uncover areas where less information was available, and then once the gaps in knowledge were validated by the website analysis, the results of the semi-structured interviews began to add new knowledge to this area. Chapter 6 now presents a coherent discussion of the findings obtained from the exploratory data analysis, website content analysis and systematic review of the academic and practice literature. The following sections present the discussion of the results detailed in Chapter 5. Using thematic analysis, macro and micro themes are identified and linked back to existing academic and practice literature to understand in depth the relevance of the emergent findings to the context investigated. The final section of the chapter discusses the implications of the findings from the theoretical, practical, methodological, social and societal perspectives and states possible avenues for future research directions.

6.2 Identified Macro Thematic Categories

In order to discuss the findings obtained in this study, each section of the interview questions was grouped into thematic interpretations and data and then presented using thematic matrices (Miles & Huberman, 1994). Grouping the questions visually allows for simple interpretation of more complex qualitative data. This grouping then allows for the common themes to be exposed, and allows for a thorough understanding of how emergent themes relate to the two dimensions of macro and micro thematic categories and their relative importance (Miles & Huberman, 1994).

Table 6.1 presents the macro thematic categories attributed to the questions asked in Section 1 of the interview questionnaire. The table also displays the number of times a response was mentioned by respondents (in brackets). Unsurprisingly, the categories of threat (n=42) and risk (n=28), including the ownership of that risk (n=34), feature

prominently. The category of motivation is somewhat tied to risk and threat, but the approach and method of action raise some interesting viewpoints. Communication was raised by four participants as they detailed the lack of information regarding their organisation cyber security plans and approaches.

Table 6.1

Macro Thematic Categories for Questions in Section 1

Questions – Individual skills and capabilities	**Macro themes**
Do you consider DDoS to be a real threat to your organisation?	Threat (n=30)
What cybersecurity event would you consider to be a greater risk?	Risk (n=28)
	Threat (n=12)
Are there any formal contingency plans in place within your organisation to mitigate the DDoS attacks in the future?	Method (n=6)
	Risk ownership (n=4)
Can you describe the steps taken to build these plans?	Approach (n=12)
	Method (n=10)
	Risk ownership (n=30)
What was the motivation for your mitigation plan?	Motivation (n=27)
	Communication (n=4)

Table 6.2 shows macro thematic categories attributed to the questions asked in Section 2 of the interview questionnaire. Risk ownership was a key theme through this section, but as the section deals with team considerations, communication (26) was a theme that was heavily discussed by the participants as, in order to construct and organise defence plans, communication with various stakeholders is required. The approach (20) taken varied, and in some cases was influenced by the relationship the organisation had with their service providers. This relationship also had an effect on the ownership of the risk (6), with a choice of dealing with the risk internally or transferring the risk to an external provider. How this occurred, along with how plans

were created and implemented, are covered by method (64), which is the largest theme in this section.

Table 6.2

Macro Thematic Categories for Questions in Section 2

Questions – Team skills and capabilities	Macro theme
Within the team, who would you say are the most important stakeholders?	Approach (n=4)
	Communication (n=7)
Is there involvement from other stakeholders (in the process), that you think are less important to those identified above?	Communication (n=9)
	Risk ownership (n=2)
What are the challenges you might face while implementing a DDoS mitigation plan?	Approach (n=1)
	Communication (n=4)
	Method (n=4)
	Risk ownership (n=4)
Have you made plans to address these challenges?	Approach (n=3)
	Communication (n=6)
	Method (n=5)
Does the existing team within the organisation have the required skills and capabilities to identify and respond to DDoS attacks?	Approach (n=12)
	Method (n=26)
How do you think your team could increase these skills and capabilities?	Method (n=29)

Table 6.3 shows macro thematic categories attributed to the questions asked in Section 3 of the interview questionnaire. This section overwhelmingly highlighted communication (n=50), approach (n=49) and method (n=47) as the dominant themes. Communication showed that organisations' and employees' perceptions could either be aligned or not, but sufficient communication was in place for participants to

comprehend the level of alignment. Communication was also closely tied to the approach and method theme, with participants discussing the importance of sharing experiences in order to transfer knowledge and enable greater learning. With regard to organisations' future plans, the method of approach and implicit capability were also seen to be prominent subjects in participants' responses. Risk ownership looks at the role each area plays and how collaboration between organisation, industry and government could improve defence capabilities.

Table 6.3

Macro Thematic Categories for Questions in Section 3

Questions – Organisational plans and motivation for capability	**Macro themes**
Do you think the organisation considers the threat of DDoS attack as more, less or the same as your own level of threat assessment?	Communication (n=21)
How has the organisation's threat perception changed over the last few years?	Communication (n=29)
How do you think the organisation could enhance the teams' future skills and capabilities to tackle DDoS attacks?	Approach (n=19)
Do you think this is the responsibility of the organisation?	Method (n=7)
	Risk ownership (n=18)
What do you think is the role of industry?	Approach (n=22)
	Method (n=22)
What do you think is the role of government?	Approach (n=8)
	Method (n=18)

6.3 Identified Micro Thematic Categories

Building on the macro themes derived in Section 6.2, each identified macro thematic category is further dissected to consider the micro themes of relative importance that were uncovered during the transcription of the interview data obtained from the participants. Table 6.4 shows the relationship between the identified micro thematic categories and their macro thematic counterparts that were attributed to the questions asked in Section 1 of the participant interviews. Threat and risk are shown to have the

largest set of micro themes even when split into two separate groups, with threat concerned with the possibility of an attack and risk more associated with the consequential outcomes. All others, including risk ownership and motivation, almost sit as attachments to these themes as these themes may be immaterial without the context of risk and threat. However, of these, motivation may influence the themes of method, ownership and communication, as differing types of motivation may require differing types of mitigation controls.

Table 6.4

Macro to Micro Thematic Relationship for Questions in Section 1

Questions – Individual skills and capabilities	**Macro themes**	**Micro themes**
Do you consider DDoS to be a real threat to your organisation?	Threat	Experience (n=7)
		Perception (n=29)
What cybersecurity event would you consider to be a greater risk?	Risk	Vandalism (n=1)
		PII-PCI-PHI (n=10)
		Loss of intellectual property (5)
		Infrastructure compromised (n=1)
		Data loss, theft (n=15)
		Reputational loss (n=6)
	Threat	State terrorism event (n=1)
		Social engineering (n=7)
		Ransomware (n=6)
		Phishing (n=5)
		Malware (n=1)
		Insider attack e.g., rogue admin (n=3)
		Human error (n=6)
		DDoS (n=1)
Are there any formal contingency plans in place within your organisation to mitigate the DDoS attacks in the future?	Risk ownership	Own plan (n=17)
		Transfer the responsibility (n=9)
		No plans (fearless) (n=5)
Can you describe the steps taken to build these plans?	Approach	Specific defence (n=5)
		Part of general defence plan (n=7)
	Method	Build from own experience (n=6)

Questions – Individual skills and capabilities	Macro themes	Micro themes
		Follow established cyber security frameworks (n=4)
	Risk ownership	Internal team (n=7)
		External expert (n=2)
		Rely on vendor (n=1)
What was the motivation for your mitigation plan?	Motivation	3rd-party pressure (customer /market expectations) (n=5)
		Own experience/fear (of attack/consequence) (n=19)
		No plans (fearless) (n=3)
	Communication	Uniformed of plans (n=4)

Of the risks, the risk of data loss featured heavily, including the loss of PII, PCI and personal health information (PHI). This fear of loss was not only concerned with the loss of proprietary data and intellectual property, but also with the loss of third-party information, including sensitive customer information, which may lead to future business loss from any incurred reputational damage. DDoS was not considered the greatest threat by many, and of the 30 interviewed, only six had personally experienced an attack. Despite this, most (n=25) considered DDoS to be a credible threat. As this perception was not created though personal experience for most of the participants, it must be acquired via external influences. That is to say, participants must build their perceptions from information delivered by peers and the information published by individual experts and organisations. This reliance on external influence to determine the level of threat does not appear to follow through to organisations' approaches to mitigation. Despite the existence and availability of several cybersecurity frameworks, most participants stated that their organisations rely on in-house experience and capability and find their own strategies for defence. This again demonstrates a reluctance to collaborate and a resistance to information sharing even when there are potential benefits such as building on the experience of others.

Table 6.5 shows the relationship between the identified micro thematic categories and their macro thematic counterparts that were attributed to the questions asked in Section 2 of the interview questionnaire. Again, participants expressed their preference to rely

on internally developed capability, and internal communication formed a key aspect of the defensive plans. Although one participant stated that their cybersecurity team operated covertly from the rest of the organisation, the majority saw benefit in information dissemination even if it remains within the organisational boundaries. Information and internal collaboration were highly valued, such that education and learning of processes and technology were highly desired, even if that opportunity was currently unavailable. Eighteen participants mentioned the need for more training, with a further eight asserting the need for more collaboration with an experienced and diverse pool.

Table 6.5

Macro to Micro Thematic Relationship for Questions in Section 2

Questions – Team skills and capabilities	Macro Themes	Micro Themes
Within the team, who would you say are the most important stakeholders?	Communication	Internal team (n=4)
	Approach	Planned response (n=5)
		Reactive, ad-hoc (n=1)
Is there involvement from other stakeholders (in the process) who you think are less important than those identified above?	Communication	Notification (n=9)
	Risk ownership	Transference (n=2)
What are the challenges you might face while implementing a DDoS mitigation plan?	Approach	Cost (n=1)
	Communication	Internal challenge (n=2)
		External challenge (n=2)
	Method	Use existing technology (n=3)
		Research new technology (n=1)
	Risk ownership	Reduction (n=2)
		Transference (n=2)
Have you made plans to address these challenges?	Approach	People (n=1)
		Process (n=1)
		Technology (n=1)
	Communication	Information dissemination (n=6)
	Method	Internal engagement (n=3)

Questions – Team skills and capabilities	Macro Themes	Micro Themes
		External engagement (n=2)
Does the existing team within the organisation have the required skills and capabilities to identify and respond to DDoS attacks?	Approach	Reliance (n=6)
		Capability (n=9)
	Method	Experience (n=23)
How do you think your team could increase these skills and capabilities?	Method	Training (n=18)
		Collaboration (n=8)
		Diversity (n=4)

Table 6.6 shows the relationship between the identified micro thematic categories and their macro thematic counterparts that were attributed to the questions asked in Section 3 of the interview questionnaire. This group of questions considered the role each area played in defending against the DDoS threat. Without good communication, alignment of thought would be optimistic, so with 23 of the participants believing there was alignment of threat perceptions between the organisation and the employees, the majority of the organisations' internal cybersecurity communication must be effective. However, these perceptions were not built in isolation. According to the participants, the role of industry and government is one of education, collaboration and governance. Education from government enables wider dispersal of gathered knowledge and intelligence, which in turn provides a greater opportunity for increased preparedness. Industry-led education delivers knowledge from the source and includes awareness of new technology applications as well as experience of practical applications and adoption of frameworks and processes. From an individual point of view, education of employees can improve their risk and threat awareness as well as their capability to implement an appropriate defence. The further empowerment of these capable and experienced employees can bring an increased level of autonomy that further improves the speed of response.

Table 6.6

Macro to Micro Thematic Relationship for Questions in Section 3

Questions - Organisational plans and motivation for capability	Macro themes	Micro themes
Do you think the organisation considers the threat of DDoS attack as more, less or the same as your own level of threat assessment?	Communication	Alignment (n=23)
How has the organisation's threat perception changed over the last few years?	Communication	Influence (n=29)
How do you think the organisation could enhance the teams' future skills and capabilities to tackle DDoS attacks?	Approach	People (n=14)
		Process (n=9)
		Technology (n=7)
Do you think this is the responsibility of the organisation?	Method	Staff empowerment (n=7)
	Risk Ownership	Training (n=7)
		Collaboration (n=8)
		Diversity (n=4)
What do you think is the role of industry?	Method	Training (n=9)
		Collaboration (n=15)
		Diversity (n=3)
	Approach	Technology (n=8)
What do you think is the role of government?	Method	Training (n=4)
		Collaboration (n=14)
		Diversity (n=2)
	Approach	Policy (n=6)
		Governance (n=6)

6.4 Thematic Relevance to Literature and Discovery of New Findings

Identification of the macro and micro themes in Sections 6.2 and 6.3 began to reveal new insights, and a natural grouping of themes was formed to simplify the discussion given that commonalities were observed in the macro and micro thematic categories

presented in the above six tables. Four larger groups of themes were formed due to their common dependencies.

1. Threat, risk and risk ownership – Threat and risk are intrinsically linked; however, ownership adds a perspective dimension to the conversation.
2. Approach, method and technology – Approach directed the method to be used, but that method may be heavily influenced by any technology available.
3. Capability and communication – Isolated capability can be sufficient, but when collaboration occurs between groups through proficient communication, whole-of-team capability can be amplified.
4. Motivation and COVID-19 – Organisations are motivated by many forms of need, and COVID-19 has been a sudden and unexpected factor to consider since late 2019.

6.4.1 Threat, Risk and Risk Ownership

Answering the initial research question, "How high do Australian organisations rate DDoS as a threat when compared to other cybersecurity events?", the results of this study indicate that, while DDoS is considered a realistic threat by staff in organisations, it falls short of being the greatest perceived threat. The greatest threat was perceived to be events that cause loss of data and/or intellectual property, especially if that data are in the form of PII, PCI or PHI information. In contrast to event outcomes that impact on productivity, organisations place particularly high importance on the loss of this type of information due to the social risk and consequences that exposing this sensitive information to unauthorised viewers can create.

Over the past decade, there have been many examples of high profile companies losing control of information within their care (Bowman, 2021; Fipps, 2018; Lord, 2016; Sharwood, 2021), and the consequences have led to (amongst others) a loss of organisational reputation (Kamiya et al., 2021). This may be the loss that companies fear most as the study showed that these types of outcomes impact on their ability to do future business in addition to the problems endured in the immediate crisis and closely after (Kamiya et al., 2021). Therefore, organisations employ a range of responses to perceived risks, and they often do this using a risk framework. For a given

risk, a common framework currently in use combines the perceived level of likelihood with the perceived consequence of the encounter should the event occur (Table 6.7).

Table 6.7

Risk Heatmap of Consequences

Likelihood of consequence	**Severity of consequence**				
	1 Insignificant Inconvenience - No time or financial loss	**2** Minor inconvenience - <1hr or $1,000 loss	**3** Moderate inconvenience – 1–4 hrs or $1k–10k loss	**4** Major issue - 4-8 hr or $10k–50k loss with reputational damage	**5** Catastrophic - >8 hr or >$50k loss with reputational damage
1 - Rare - Only in exceptional circumstances	1	2	3	4	5
2 - Unlikely - Has occurred once in the last 3 years	2	4	6	8	10
3 - Possible - Has occurred once in a year	3	6	9	12	15
4 - Likely - Has happened two or more times/year	4	8	12	16	20
5 - Almost certain - Has happened many times	5	10	16	20	25
Risk Rating - Likelihood * Severity	Minimal 1-2	Low 3-9	Medium 10-15	High 16-20	Extreme 25

Note. Adapted from Chapelle (2019)

The measure of likelihood could be rated by methods such as using an expert's opinion or considering historical statistics that detail the number of previous occurrences over time (University of Melbourne, 2018b). Similarly, consequence may be rated using methods such as financial cost or the severity of impact on human life (University of Melbourne, 2018). In this way, how the risk is assessed depends on the type of risk being considered. The approach to how likelihood and consequence are measured can be classified into three categories: a psychological approach, an

anthropological/sociological approach, or a combination of these through an interdisciplinary approach (Lavino & Neumann, 2010).

The psychological approach combines heuristics and cognitive psychology, where heuristics is the use of short cuts in thinking, such as similarity assessments and bias towards more easily recalled ideas, and cognitive psychology includes the use of motivation, problem solving and decision making (Neset, 2018). The anthropological/sociological approach suggests that cultural theory perceptions of risk are influenced by social constructions, cultural values and ways of life (Wildavsky & Dake, 1990). One way to aid understanding of this complexity is to build a risk rating table (Table 6.8). Assigning a value to each of the likelihood and consequence options in the risk heat map (Table 6.7) then multiplying these two values gives a score that is then used with a risk rating and control table (Table 6.8) to establish the risk rating for the risk. Cox (2008) believes this method to be error prone as two risks may be calculated to have the same risk score, but in reality they have disparate outcomes that may lead to an inappropriate response. However, if this potential inaccuracy is acknowledged when interpreting results, when combined with existing control measures, the risk rating can set the approach to risk management.

Table 6.8

Risk Rating Table and Control Actions

Score	Risk level	Action
Score 1–2	Minimal risk	Maintain existing measures
Score 3–9	Low risk	Review existing measures
Score 10–15	Medium risk	Improve existing measures
Score 16–20	High risk	Review approach
Score 25	Extreme risk	Immediate action required

Note. Adapted from Chapelle (2019)

While this is one acceptable form of risk assessment, there are other frameworks that businesses use in their risk assessments, such as PESTEL and SWOT. PESTEL is an

extension of the PEST framework (Kotler et al., 2013) and is a framework that allows organisations to examine factors that may impact on business from six perspectives: political, economic, social, technological, environmental and legal (De Bruin, 2016). Each domain attempts to split the overall threat landscape into describable areas for consideration.

Political factors may include economic policy changes, trade relationships and taxation (Shatskaya et al., 2016). Political factors remain a necessary but uncontrollable aspect. Some extremely large organisations may have the ability to influence political direction (Drury, 2022), but for the most part, political policies are determined by a small group of elected officials (Department of the House of Representatives, 2018). Economic factors that affect the economy can include direct influences such as interest rates and currency exchange rates and indirect influences such as material costs and employment rates (Shatskaya et al., 2016). While some of these may be influenced by political policy, many factors react to the changes that occur in other areas. For example, the 2019 COVID-19 pandemic influenced economic capabilities due to the various restrictions that were put in place and the direct impact on individual health (Munawar et al., 2021).

Social factors would also consider the pandemic affects but should consider other more general emerging trends and various social demographics such as family, education and lifestyle changes (Shatskaya et al., 2016). Environmental factors such as climate and the carbon footprint are especially relevant in 2022 as Australia increases its focus on the SDGs (UN, 2022). Legal factors do have some crossover with political factors as legislation is created by political agencies; however, unless policy becomes legislation, there are no compliance requirements (Department of the House of Representatives, 2018). Policies are guiding principles, whereas legislation are rules that must be complied with (Department of the House of Representatives, 2018). As such, the legal factors include consumer law, health and safety, privacy and other enforceable legislation. PESTEL's technology factor is where cybersecurity should be addressed, as it considers how trends in the digital landscape may change over time and how these new opportunities may also open up new areas of potential weakness.

A SWOT analysis can also be used for risk assessment, where strengths, weaknesses, opportunities and threats (SWOT) are all considered relevant for helping organisations to formulate a strategy to cope with potential events (Humphrey, 2005). With a SWOT analysis, strengths and weaknesses are considered to be able to be managed internally whereas external influences are recorded as opportunities and threats. This split between external and internal influences is where alignment exists between PESTEL and SWOT. As shown in Figure 6.1, the P,E,S,T and L elements of PESTEL all contribute to SWOT threats and the P,S,T and E elements provide potential opportunities for the organisation to exploit. For example, the external influences, political factors (P) and social factors (S) are unlikely to constitute a strength or weakness but can present opportunities or threats.

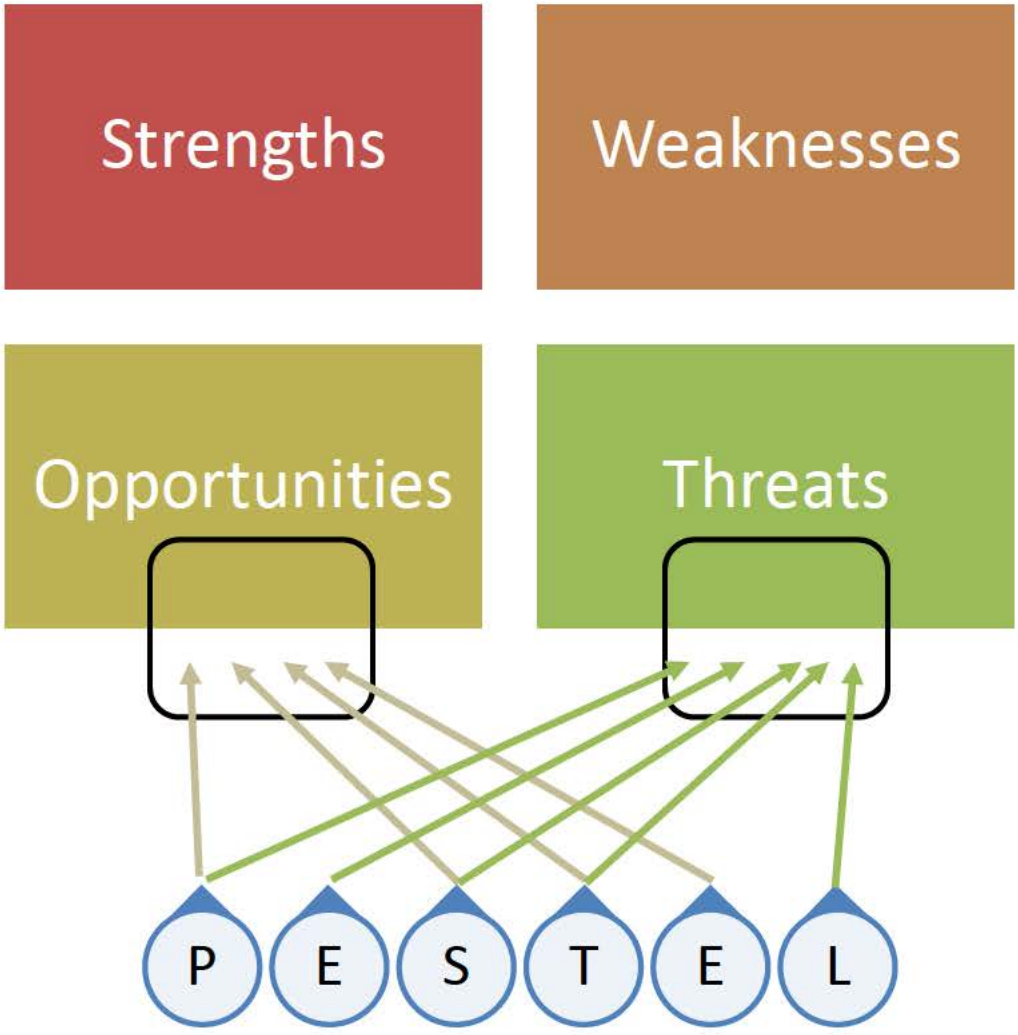


Figure 6.1. SWOT and PESTEL alignment (adapted from Del Marmol et al. (2015) and Helms and Nixon (2010))

However, despite the availability of several existing conventional business risk frameworks, new cybersecurity-specific frameworks are becoming more widely used, and these frameworks must accommodate the types of risk that cybersecurity should consider, such as ethical, security, privacy and technical risks (Kandasamy et al., 2020). The National Institute of Standards and Technology (NIST) promotes a USA-led framework for cybersecurity (Joint Task Force, 2018). In this framework, risks are assessed and allocated a treatment method based on an assessment of the outcome. These could be:

- Accept the risk if the outcome is free from harm.
- Mitigate the risk through the application of security measures.
- Transfer the risk to another responsible party.
- Avoid the risk, including potential removal of the device.

Operationally, critical, threat, asset and vulnerability evaluation (OCTAVE) is another USA-developed framework that proposes eight steps that should be employed as cyber-threats are evaluated (Kandasamy et al., 2020).

1. Set up the criteria to measure risk.
2. Develop the asset profiles.
3. Identify the asset containers.
4. Identify the areas of concern.
5. Identify any threat schemes.
6. Recognise the risks.
7. Examine the risks.
8. Mitigate the risks.

The International Electrotechnical Commission (IEC) and the International Standards Organization (ISO) jointly released the ISO/IEC 27001 set of standards for information security with the intent of setting out an international standard for the assessment of cyber risk (Wu et al., 2022). However, the Australian Government recommends using their Essential Eight maturity model (ACSC, 2021), which allows organisations to self-assess their cybersecurity maturity and assign a maturity level from zero to three in consideration of the type of attackers that are likely to be a threat against eight strategic segments.

- Maturity Level Zero – Weaknesses exist that could allow compromise or

impact on the integrity or availability of systems and data.

- Maturity Level One – Security controls are focused on mitigating attacks from opportunistic adversaries using common exploits, stolen credentials and spam/phishing attacks.
- Maturity Level Two – Security controls are focused on mitigating attacks from adversaries who are targeting the organisation using account impersonation and other advanced techniques to bypass organisational security while avoiding detection.
- Maturity Level Three – Security controls consider the threat from advanced adversaries who are willing to spend a lot of time and effort to exploit any vulnerability to obtain or disrupt organisational data during storage and transmission while evading detection.

A common element in these frameworks is that they all seek to demystify and remove the complexity from cybersecurity assessment, as assessment is the first important step in the path of effective cybersecurity (Ibrahim et al., 2018; Fulford, 2020). If an organisation wants to know how to get to its cybersecurity goal, it must know from where to start

With all the frameworks available to organisations and with the push from the Australian Government for organisations to be cyber secure (Hendry, 2021), it is surprising that only 17 of the respondents said that their organisation had a formal plan. The organisations of nine of the respondents had no plan (four were unaware of any plan), so how do those organisations expect to continue business if an attack were to occur?

Avoid

Of the mitigation methods reported across the interviewed pool, three categories of mitigation were accounted for: reduce, accept and transfer. Only the mitigation option of avoid was not present, which could be critical for organisational planning for the future. Avoiding a risk can include the development of an alternate strategy, potentially at a higher cost or reduced efficiency. This method may also include the use of proven technology rather than cutting edge technology adoption, which could provide increased performance at lower costs. However, at its extreme, removal of a

risk would be the most effective, as is seen in the control approach to extreme risks, where the control action may be to not proceed (See Table 6.8). This option may be very difficult to achieve, as much of the business requires the use of, or is conducted through, networked computers and devices. Given a DDoS cyber-attack requires a motivated person, a reachable target and a compromised botnet and that the initial two factors sit outside the target organisation's reach of influence, target removal may be the only option. Thus, avoidance as a mitigation risk control may prove to be impractical and therefore not an option considered by organisations of the interviewed participants.

Reduction

Risk reduction can employ many forms, including engaging partners with higher levels of expertise, distribution of service capabilities, removal of single points of failure, implementation of advanced technology solutions and proactive strategies such as offline backups of systems and data. Depending on the method employed, the mitigation technique can be costly as it may involve the duplication of production architecture. As such, where this strategy is employed, organisations often seek to duplicate a subset of the entire infrastructure and a risk analysis process is undertaken to understand which systems and at what capacity the failover architecture should be considered. This method is not restricted to technology. People can also be vulnerable and, as such, organisations make provision for loss or incapacity, but this requires the development of processes that can be followed by replacement staff and application of access rights to roles rather than the individuals themselves (Ferraiolo et al., 2007).

People can also be part of the mitigation strategy. Two interview participants commented on the development of security and network operations centres (SOC/NOC) that would be available to facilitate the early detection and manual intervention of cyber events, while another commented on the fall-back option of reverting to manual processes if digital systems become incapacitated. While both options can be part of a valid cybersecurity program, both also rely heavily on manual effort and high labour costs and may not produce consistent and repeatable results.

Accept

In some cases, following a risk assessment process, specific systems may be considered to be less of a priority. This includes systems that can easily be worked

around with alternate processes as well as those where the architecture makes acceptable cybersecurity an impractical option. In these cases, organisations may choose to accept the risk and deal with the consequences. Additionally, "accept" is also a method chosen by some organisations that have transferred their platforms, software and infrastructure to cloud service providers. In these cases, and as stated by two of the interviewees, there is a belief that following successful cloud migration, the cloud providers assume the responsibility for cyber defence; however, generally speaking, the cloud provider is only responsible for securing the cloud infrastructure, leaving the customer responsible for securing the applications and data they store within that cloud (AWS, 2022; Google, 2019; Lanfear & Berry, 2022). The organisation accepts the consequence of any cyber-attack that successfully overcomes the cloud provider's defences if any are provided, which, as shown, is not always the case.

Transfer

While migrating systems to a cloud environment can be a form of an accept mitigation, it could also be considered a transfer mitigation. Risk transfer can include recognisable methods such as insurance. Cyber insurance protects an organisation in several ways: covering the costs involved in responding to a cyber-attack, covering third-party liability should a data breach occur, whether it is caused by external attack or internal theft, and professional indemnity against errors and omissions when providing digital services (Franklin et al., 2009). Although the increase in nation state type attacks may affect the outcome of an insurance claim as these attacks may be considered an act of war and thus not covered by policies (Chaudhry, 2022). Another method of risk transfer is the use of internal and external expertise. Along with a move to cloud, external expertise could also include the use of specialist technology vendors who manage organisations' security implementations.

Planning risk or frameworks

Those interviewed participants who reported that their organisation had made plans to mitigate cyber-attacks discussed the methods of risk assessment utilised, and much of the discussion revolved around traditional risk assessment approaches. While there was mention of frameworks such as NIST and ISO 27001, very few discussed using these frameworks in their process of assessment in any detail, whereas those that used

conventional methods were more at ease with the discussion. This may be because of the relative newness of these frameworks compared to the traditional counterparts, so participants may have felt uncomfortable discussing a topic where they lack depth of knowledge. Alternatively, it could be driven by the unwillingness to share valuable knowledge and experience that could be a key source of competitive advantage.

Alignment

Most participants were aligned with the organisation in terms of threat perception, but employees are not restricted to only the information the organisation, industry and government provides them. As such, any difference in alignment could be explained by staff having access to multiple forms of information from a diverse pool of information sources. They can take organisation-provided information and blend it with the information they personally gather from a wide range of sources, and this mixture could give an infinitely diverse result.

The consequence of an attack is a significant factor in how a threat assessment is estimated. The alignment of organisations and participants can be useful, as having the organisation and employees in tune allows organisations to move forward with plans more easily (Alagaraja & Shuck, 2015), but diversity of thought is a valuable asset when working to develop new innovative methods. Therefore, having a wider range of views may lead to a more beneficial outcome.

While more information has been uncovered, there are still unanswered questions. Despite most participants agreeing that DDoS is a credible threat, many of their organisations lack formal contingency plans. Understanding why this is may help to develop more effective ways of engagement. It is possible that those organisations without plans may have transferred the risk to other partners, but this is difficult to ascertain as no evidence of partnerships was found in the website analysis. This may be because there are none, or perhaps because organisations wish to limit public knowledge of their strategic alliances through fear of compromise. It is also possible that some organisations may view any consequence of a DDoS attack as a trivial experience. While the impact of an attack may incapacitate a target during an attack and affect the organisation's future business reputation, the inability to do business may be short lived and consequential reputational damage may start to fade from

public memory in the weeks and months following the cyber event. In any case, these are still unexplored areas of knowledge that need further investigation.

6.4.2 Approach, Method and Technology

Not all organisation's follow the same approach to bring cyber defence to their desired standards. Some prefer to plan, while others fall into a reactive position and this variance can lead to differences in the methods undertaken and, the technology chosen, including the way that technology is applied and used.

6.4.2.1 Approach

When considering DDoS defence, the study participants stated that their organisations considered a strategic or tactical approach. Those organisations that chose a strategic option had formed a view of the organisation's security posture then handed down a strategic outcome for the relevant technology department to delivery. The tactical approach was commonly in reaction to a specific threat, which highlights that these approaches are much more focused on the near term than their strategic counterparts. However, both groups arrived at their decision by relying on information gathered from industry and government sources combined with first-hand experience. While the first research subquestion asks how the threat was evaluated, an organisation's approach to cybersecurity may already be in place prior to this question being raised. Two of the approaches to cybersecurity could be classed as risk based and maturity based.

Risk-based approach – In this study, those organisations that followed a risk-based approach (approximately 50%) easily outweighed all other choices. In a risk-based approach, organisations consider the value of the asssets they hold against the potential threats that may seek to disrupt those assets and their operations. Muckin and Fitch (2019) discuss a difficulty with this approach within organisations. As common organisational structures separate design, development and release teams from the teams that take ownership of operation, system design is often lacking vital up-to-date threat intelligence and operational teams are slow to evolve their capabilities and security posture. While the proposal by Muckin and Fitch (2019) to move to a dev-ops style approach would provide improvements to this challenge, accurate information on potential threats and associated risks are still required to create a cybersecurity project's value proposition and to help a business agreement to proceed.

Riskbased approaches such as ISO27001 (ISO, 2021) are easily assessed against cost, and cost is a value that is well understood by business. However, knowledge of threats can only be built through historic events, and risk assessments are performed using educated predictions for future possibilities. As such, future predictions suffer inaccuracies in the likelihood of a known event occurring and in the likelihood of an unknown event becoming a reality. Unknown events are particularly difficult to assess and value and, therefore, much more difficult to justify.

Maturity-based approach – The maturity-based approach, which has been adopted by the organisations of three of the respondents, requires evaluation of information known to the organisation. However, it relies on the assessor's own interpretation, which can lead to inconsistencies in results. The ACSC's (2021) Essential Eight is a maturity-based approach. Its four levels of maturity (Levels 0–3) cover the most basic aspects of an organisation's security considerations: rights of access to information, application control, patch management, information protection and authentication. Organisations are required to self-assess their level of maturity against a list of recommended procedures, techniques and tools, with higher maturity levels potentially providing more protection than lower levels. This method relies on the accuracy and honesty of those performing the assessment to achieve an accurate report. However, even the highest level of assessment using this model does not guarantee protection, as the model references rate maturity, which may not necessarily correlate to defence capability. While cyber-security practitioners may find this model provides a simplistic method to demonstrate improvements, organisations may find it difficult to determine precise value and accurately cost the effort involved in moving between levels, which may explain the relatively low adoption of this approach.

Reactive approach – Of course, an organisation may choose to ignore these options altogether and be reactive. With this method, an attack event causes organisations to react and seek to overcome or absorb any consequential loss before moving to the recovery phase. Once the attack has been dealt with, new plans and mitigations may be implemented, but as these are based on first-hand experience, strategies and tactical plans can be more closely matched to the individual business concerned. This provides an advantage as they may be well trained to combat replications of previous attacks,

but a downside to this strategy is that they may not be as well prepared for new or as yet unknown events.

Transference – A fourth approach is one of denial and transference. Several of the interviewees either believed their organisation would not be a target or, if they were, it had already transferred responsibility of the defence to a third party, such as their chosen cloud provider. This perception of not being a valid target assumes that all cyber-attacks are the result of selective targeting. However, recent data show that major targets for DDoS attacks are health care, technology and telecommunications (Warburton, 2021), and while notable large DDoS attacks were reportedly undertaken by highly capable attacking groups against large, well-known brands, there are many attacks that are performed by smaller groups who favour an opportunistic approach (Vijayan, 2020). Therefore, given the randomness of target selection, any perception that a business is too small or not part of an industry worthy of attack is an invalid argument.

Cloud migration – Organisations that have migrated systems to cloud providers may have aligned their threat profile with well-known potential targets. Large companies such as Google, AWS and Microsoft could be seen as high-profile targets, with smaller customer organisations being a casualty of a directed attack at their cloud organisation's infrastructure (Spadafora, 2020). Additionally, while the risk may have been transferred to the cloud provider, any damage will likely still sit with the organisation themselves. Any loss of confidential data could be damaging to organisational reputation irrespective of who is ultimately found to be at fault.

Regardless of the approach option selected, how an organisation manages its software and hardware using controls such as policies and processes heavily influences the success or failure of their cybersecurity defences. Each area could be addressed individually, as while capable defences in some areas protect vital information, failure in other areas could prove catastrophic. Therefore, the collective term 'cybersecurity posture' is a more valid descriptor of an organisation's cyber defence capability.

6.4.2.2 Method

While the approach looks at what an organisation wants to achieve from improving their security posture, there are differing methods by which these visions could be achieved. In the interviews, the respondents offered two examples:

1. To use first-hand experience and build defences against attacks known to have occurred and those predicted as likely to occur with a high degree of accuracy, or
2. To follow guidelines suggested by one of the cyber security frameworks, such as ISO 27000, ASD, NIST or the Protective Security Policy Framework (PSPF).

Experience – Conceptualising these two methods, they could be considered as relying on personal experience or the trust of expert guidance, the choice of which is made by those in command. In the case of first-hand experience, it could be suggested that sufficient experience could create an expert in one's own individual circumstances. However, measurement of expertise is subjective, and the same perceptions of expertise also apply to authoritative groups. From a distance, it is difficult to understand the level of expertise of the individuals that created these promoted frameworks. The measure of expertise should be assessed through the outcome of a tested solution, which can only be achieved in hindsight. In addition, evidence of past performance is no guarantee of future results. Therefore, the difference between these two methods lies elsewhere than simply a measure of expertise.

Framework – Between methods, differences exist in the level of detail considered. Those with first-hand experience can consider micro levels of detail within the narrow context of the organisation itself. Ideas, theories, plans and measurements are conceived and implemented within the sphere of organisational authority. By contrast, the construction of universal frameworks considers a broader view across multiple industries and combines input from multiple individuals with diverse experiences. Consequently, these frameworks adopt a more generalised view and lack the ability to consider individualised complications.

The optimal path is likely to sit within the overlap of these two methods (Figure 6.2), where an overall framework would guide the efforts, but a degree of personal experience would be used to adjust the application method.

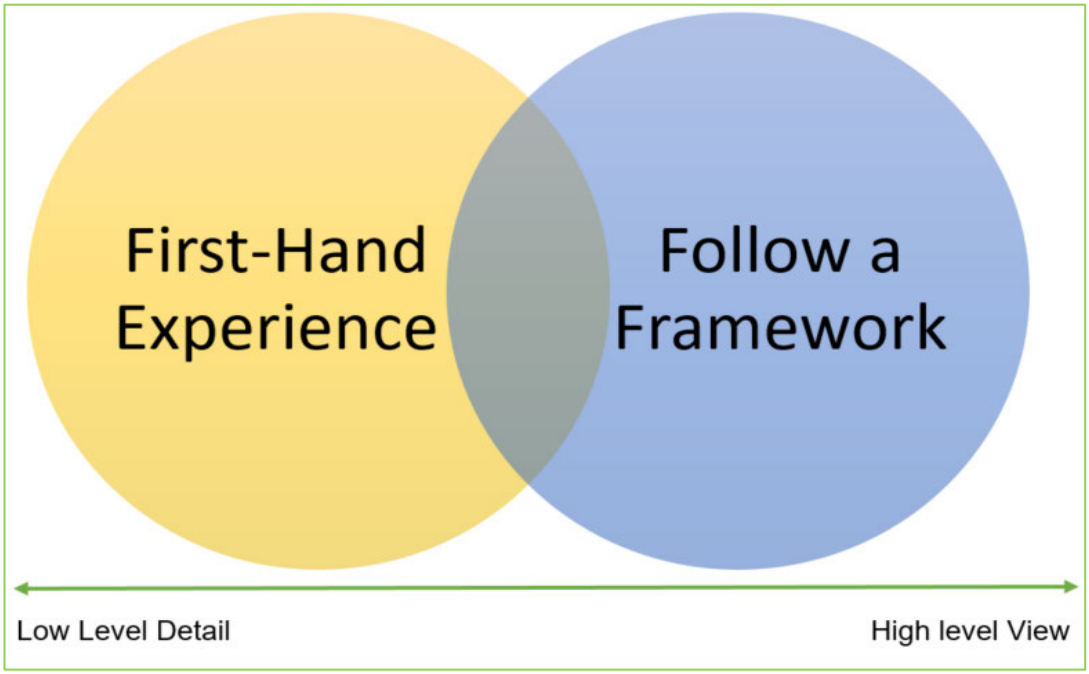


Figure 6.2. Method comparison (by researcher)

Similar observations were made during the interviews. Several interviewees indicated that their organisation intended to follow a prescribed framework, as doing so would improve their security posture while also providing the ability to ensure stakeholder acceptance of the strategy due to the implied quality of conforming to a socially accepted standard. However, the implementation was often easier when prior cyber-attack experience had occurred, as previous experience not only facilitated support for the proposal, but also enabled the project teams to customise the delivery to areas where they believed improvements would have most effect. This also supports the knowledge gained from the literature review, as if individual motivations can be shaped by culture (Hofstede et al., 2010), it is possible that professional motivations could be shaped by organisational events.

These two methods are driven from within organisations. Further alternatives could be through actions driven by external groups. These alternative options include:

- The availability of cyber-security training and certification offered by academic and professional learning providers.

- Governments mandating alignment with frameworks such as the Essential Eight cyber maturity model (Anderson, 2021).
- The follow-on impact of third-party vendors' own implementation of cyber defence.

6.4.2.3 Technology

Cyber defence relies on three interconnected factors: people, process and technology. The people aspect can be somewhat fluid as individuals can apply technology in infinite ways and adjust how closely they follow processes with their free will. This adaptability and flexibility in their approach to how processes and technology are applied is what influences the variance in the outcomes achieved. However, the process and technology parts (in the absence of machine learning) can be somewhat innate, as once configured and left untouched, they remain consistent.

The choice of technology is a decision made by groups and individuals, and their choice can vary between products with different security features, including options that are absent from any security features. In addition, the configuration of these devices can have a significant effect on the result, as those with more expertise may have more understanding of the complex technologies involved. The ultimate choice of the technology products adopted may be a risk the decision maker is willing to take. However, due to the connectivity of these devices, the risk and consequence of this selection may be felt more widely.

In Australia, as of December 2021, minimum standards for cybersecurity in internet-connected devices do not exist. Network-capable products may or may not have cybersecurity features, including passwords, firewalls or access control lists (ACLs). Many devices still operate with simple, well-known passwords (Shadman, 2017), such as the security cameras that were heavily involved in the 2016 Mirai DDoS attack (Vlajic & Zhou, 2018).

Standards – Issues with product standards were raised in the interviews. The Australian Consumer Law governs product quality, ensuring fairness between retailer and consumer (Australian Consumer Law, 2016). This law directs minimum levels of safety as well as consumer satisfaction for all products available in Australia; however, it fails to specify information directly related to the cybersecurity level or functionality

of network-capable products. According to the legislation, products must be safe to use and function as advertised, but there is no legislation to ensure that they prevent unauthorised access or control. Similarly, while the ACCC has powers to govern compliance with this legislation, the legislation has fallen behind technology and powers with respect to cybersecurity are non-existent. Bad actors remain keen to exploit the vulnerabilities of the insecure products available for purchase in Australia.

It seems that only when consumers become aware of the risks do they provoke change through purchasing preference (Blythe, 2020). Therefore, the pressure for manufacturers to develop safe and secure connected devices must be driven by sector competition and consumer preference, but this comes at a cost (Blythe, 2020). As costs to develop and implement cybersecurity features raise product prices, consumers may opt for less secure options, further expanding Australia's threat landscape. One way to prevent this would be to update consumer protective legislation with the introduction of minimum levels of cybersecurity defence or standards for internet-connected products and software. Legislation would force manufacturers to comply, which would raise their standards and deliver secure options for consumers. However, to be effective, new legislation should be jointly implemented with methods of governance and auditing compliance.

Configuration – Technology that is 'secure by design' is only one aspect of a secure implementation (Duncan, 2020). Devices that connect to networks are often highly configurable with many options for each of the security features included in the design. The choice of how these are configured may increase or decrease the level of security from the default set by manufactures, although it is often the case that initial choices are required during the device's initial configuration. Individuals who are influenced by their own threat perceptions can adjust the level of device protection as they see best fits their purpose. However, if unskilled individuals are those tasked with configuration, the resultant security outcome may be less than optimal. Therefore, if devices are manually configured, it is important that those configuring network devices have threat perceptions that are aligned with organisational decision makers.

To counter this configuration weakness and inconsistency, one option may be to encourage manufacturers to adopt more simplistic methods of configuration where unskilled users are more adequately guided through the complex configuration

process. A second option may be to automate the configuration or use AI and ML to configure the device based on analytics (Cisco, 2020). The advantages of this method could include:

- Simplified configuration – Easing the way to ensure security outcomes align with agreed organisational policy.
- Improved response to cyber events – Particularly useful in cases where IoT devices provide poor visibility of state.
- Inclusion in security framework – For cases where devices connect to networks inconsistently.
- Zero trust – Simplified implementation of the zero-trust model.

Vendors/Consultants

Some interviewees commented that a third party looked after their organisation's security, and this method has been achieved either through vendors/consultants or through cloud operators. This subsection discusses vendors/consultants, and the following section discusses cloud operators.

When considering the use of vendors or consultants the level of skill and competency of the supplier should align with the needs of the organisation. Each option, such as security providers or managed service providers, may present different strengths and capabilities but in addition, there are other consideration that may have more influence on the final choice.

Security provider – An organisation could contract a specialist security provider to take on the responsibility for their cyber defence. This could be a good strategy as the cost of employing and maintaining a cybersecurity team can be such that the cost outweighs the value. This is particularly true if the organisation is a small or medium-sized business or where the firm does not operate in the information technology sector. In IT organisations, staff with technology skills may be able to dedicate a portion of their capacity to cybersecurity workloads; however, this may not be the case in other industries, and this could mean that the full cost of maintaining a dedicated cybersecurity team is born by the organisation, even though they do not create sufficient workload to keep their defensive teams fully utilised.

Managed service provider – Transferring this responsibility to a third-party provider or managed service provider (MSP) could deliver an acceptable result at a much-reduced cost. In addition, as the MSP performs this type of work for many similar firms, their skills remain current, and experience gained from one client can be used across the whole pool of organisations they are contracted to. Another benefit of MSPs is their objectivity. As MSPs operate externally to the organisation, they can be less inclined to follow the unwritten rules of organisational propriety tradition. This positioning could provide more clarity from their objective perspective, and this may increase the adherence to formal best practice guidelines and standards. However, despite these positive benefits, several other considerations should be investigated before a decision is made to partner with an MSP. Despite the mass of information currently written regarding cybersecurity, the industry is still in its infancy relative to the industries it supports.

Skills and training – Employees with the skills and experiences to fulfil these roles are still being trained and the industry is suffering a skills shortage that may continue beyond 2022 (AustCyber, 2019). Cyber-security as a service is an emerging trend amongst MSPs, including those who have had many years' experience in providing technology environment management. As such, the level of cyber maturity actually delivered may not always be as high as assumed.

Control – A second consideration would be one of control. As an organisation has an intrinsic knowledge of the value of their data and the eminent priorities of fundamental business practices, there are likely to be some assumptions about the security focus and mitigation priorities. Equally, the MSPs running their own businesses will have a defined set of repeatable practices and replicable security strategies within their offered security product. However, these two perspectives may not be completely aligned, which means the organisation may lose control of their cybersecurity strategic goals and acquire a less then acceptable outcome.

Cybersecurity – Finally, organisations may need to consider the level of cybersecurity the MSP applies to itself. If an MSP's focus is primarily on customer cyber defence at the detriment to their own, the MSP could be seen as a potential target for a supply chain attack. One way to minimise this risk would be to adopt a certification policy that requires vendors to be certified to an acknowledged standard,

such as ISO 270001. Standards such as this require the vendor to have reached a level of cyber defence maturity and prove their ability to consistently achieve compliance with the standard through regular audits.

Cloud operators

Another third-party option for organisations is for an organisation to rely on the cybersecurity defences put in place by the cloud provider that hosts their applications and services. Cloud computing makes use of virtualisation technologies and high-speed internet access to provide organisations with distributed computer power and storage in the form of Infrastructure as a Service (IAAS), Platform as a Service (PAAS) or Software as a Service (SAAS). Each form permits differing levels of customisation and therefore each requires appropriate levels of administrative effort. IAAS provides the most flexibility as it allows the organisation to make fundamental decisions, including the virtual server specification, operating systems and a host of other configurable options. It is the distributed cloud offering that most closely matches the historical method of purchasing hardware, and the organisation is expected to manage almost everything about the private system, such as authentication and software upgrades.

Scale, distribution and some aspects of fault tolerance are managed by the cloud providers, with most of this complexity hidden from the view of the customer. At the other end of the offerings, SAAS provides an application for organisations to use. Configuration is limited to options within the application itself; however, software patching, software upgrades, backups and application performance are all handled by the vendor offering the product. PAAS sits between these two, providing managed environments for organisations to perform their own application development. Therefore, while the infrastructure, hardware and operating system are all managed by the provider, as shown in Figure 6.3, anything above the operating system layer or built within the development space becomes the responsibility of the organisation.

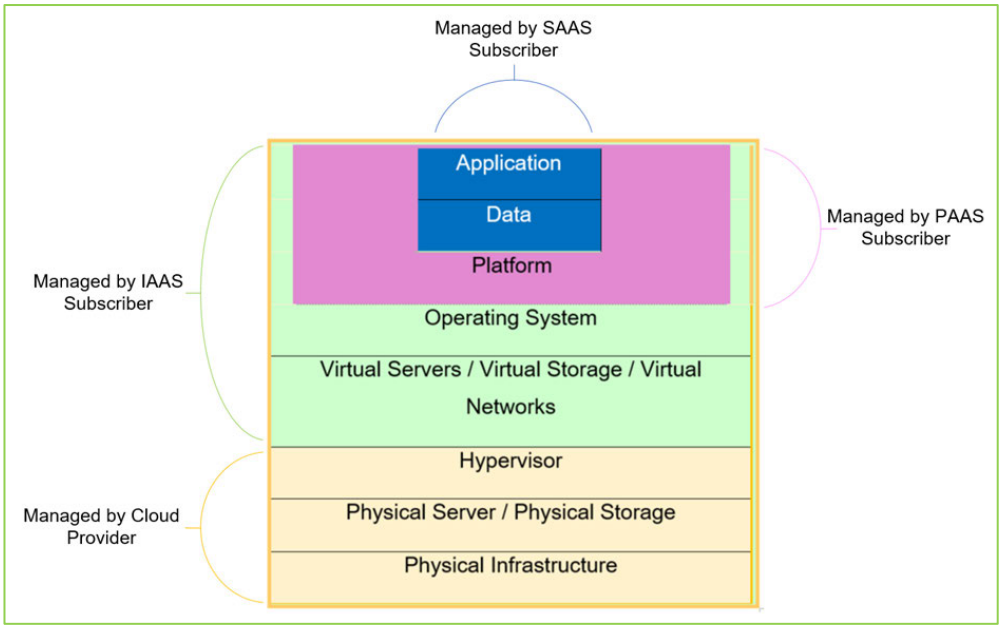


Figure 6.3. Cloud service and management responsibility (by researcher)

The boundaries between these three types of service could blur the lines of cyber defence responsibility, and the clarity of responsibility could become even more unclear when further options of in-house cloud, private cloud, public cloud, multi cloud or hybrid cloud are integrated into the overall strategy. It would also seem difficult for an organisation to transfer all cyber defence responsibility, as even with SAAS adoption, the organisation remains responsible for granting authorisation only to valid users and for the adoption of any optional security controls provided by the application vendor.

Consequence

Both options (vendor and cloud operators) bring benefits to the organisation; however, while in each case the third party accepts the responsibility for cyber defence, much of the consequence still remains with the organisation. Any failure to secure data or maintain operation is likely to be placed by customers and affected parties on the organisation itself, even if the organisation, in turn, allocates blame on the third party. This means that lasting reputational damage or loss of data or intellectual property will still be felt by the organisation even if the third party agrees to shoulder the blame. At best, this type of transference only ensures that the consequence of an attack will be shared amongst all implicated groups; organisations cannot wholly transfer the risk to someone else.

6.4.3 Capability and Communication

As organisations have a workforce larger than a single employee, capability is a measure of the combined groups' competencies, but to bring individual skills and experiences together, opportunities and ways to collaborate must also exist. In the interviews, the respondents discussed how they felt about the skill sets within their organisation and Australian industry with common themes expressed by many.

6.4.3.1 Training and collaboration

Nineteen respondents commented that more training is needed. Cybersecurity certifications have been available for many years, and more recently universities have started to offer formal qualifications at graduate and postgraduate level. A brief review of industry certification providers showed 19 potential certifications from six identified providers (see Table 6.9). In addition, universities offer postgraduate certificates and bachelor and master's degrees.

Certification – Industry certification differs to university degrees by way of topic coverage and duration to complete. Industry certificates tend to focus more narrowly and are aimed at professionals seeking to obtain evidence of their expertise in specialist areas, whereas years studying for university degrees provide richer coverage of cybersecurity principles and develop skills that are much more transferrable than those acquired in the few weeks required to acquire an industry certification. Opportunities for training are evidently substantial in the marketplace and Table 6.9 shows that roles advertised on *Seek* and *LinkedIn* indicate that employers are also seeking a subset of the available accreditations, with some more sought after than others. While the majority of respondents believed the organisation was responsible for driving education and skills increases, this overview of the employment marketplace suggests an alternate view. Those wishing to change roles or move to new employers will find the onus of training falls to the individual. As certification becomes a standard requirement for many cybersecurity and technology roles, the driving factor will become the individual's own plans to realise their own career path.

Table 6.9

Accreditation and Role Requirements

Provider	Certificate acronym	Certificate name	Seek Australia	LinkedIn Australia
CompTIA	CompTIA Security+	Security+	12	1,589
CompTIA	CASP	CompTIA Advanced Security Practitioner	0	1
ECCouncil	CEH	Certified Ethical Hacker	2	1
GIAC	GSEC	GIAC Security Essentials	15	55
GIAC	GCIA	GIAC Certified Intrusion Analyst	20	13
GIAC	GCIH	GIAC Certified Incident Handler	19	31
ISACA	CISA	Certified Information Systems Auditor	613	252
ISACA	CISM	Certified Information Security Manager	455	230
ISACA	CSX-P	Cybersecurity Practitioner Certification	1	5
ISC	CISSP	Certified Information Systems Security Professional	1,033	1,395
ISC	SSCP	Systems Security Certified Practitioner	5	13
ISC	CCSP	Certified Cloud Security Professional	20	34
ISC	CAP	Certified Authorization Professional	0	0
ISC	CSSLP	Certified Secure Software Lifecycle Professional	5	0
ISC	HCISPP	HealthCare Information Security and Privacy Practitioner	0	0
Offensive Security	OSCP	Offensive Security Certified Professional	485	88
Offensive Security	OSDA	Offensive Security Defence Analyst	0	0
Offensive Security	OSWA	Offensive Security Web Assessor	0	0
University	BCyb Security	Bachelor of Cyber Security	81	283
University	BSCS	Bachelor Science Cyber Security	2	33
University	MCyb Security	Master of Cyber Security	56	273
University	MSCS	Master Science Cyber Security	4	12
University	GradCertCybSecurity	Graduate Certificate in Cyber Security	36	5

Source: (CompTIA, 2021; EC-Council, 2021; GIAC, 2021; ISACA, 2021; Offensive Security, 2021)

Training – Formal training is a necessity for career growth and to deliver practical capability. Formal training provides employees with knowledge of concepts, methods for mitigation and detailed instruction on device-specific configuration processes. However, formal training is not the only method of knowledge transfer. The fact that formal training can take many months of planning to deliver means that in the rapidly changing world of cybersecurity, by the time of delivery, the content may already be stale. Formal training is therefore well aligned to deliver knowledge on aspects of cybersecurity that are less prone to sudden change, such as the conceptual model of an attack or the function of a device that will be present in the market for a number of years.

Collaboration – An alternative form of knowledge transfer is collaboration, and the need for this was mentioned by several respondents in the interviews. Interviewees believed vital information could be gained not only by attending training courses but also by learning from the experience of others. As this study found that minimal information is publicly released by organisations via websites, interviewees thought conferences and collaborative groups would be an effective way for first-hand experiences and lessons learned to be distributed. This has been demonstrated through the emergence of cybersecurity conferences (Cole, 2019).

In the interviews, there was variance in the perception of the validity of the threats, with 17% believing that DDoS is not a threat to their organisation, and that data loss is a greater threat. Organisations may under-report their attacks to reduce reputational damage (Britz, 2013), and there is little in the way of evidence of attacks published by the victim organisations; therefore, where this perception is drawn from is something that should be examined more deeply. The protection motivation theory (Rogers, 1983) suggests that individuals base threat perception on a mix of six factors, four of which are the severity of the event, the likelihood of the event, the preparedness of the victim, and the victim's motivation to defend. These personal understandings of risk are developed over time through social and cultural exposure and experiences, so it is possible that these perceptions are formed from a combination of personal and organisational experience and a thin slice of newsworthy events published in media reports. News agencies need to convey journalist integrity, but as a business they need to balance this with content that generates sales. As such, headline-grabbing content

is more likely to be published (Pinker, 2018), and this bias towards sensationalism could indirectly influence the threat perceptions in organisations. Therefore, collaboration that involves enabling direct access to a wider and more directly connected knowledge-sharing source may invoke a form of moderation in the volumes of cybersecurity information available.

6.4.3.2 Cultural diversity

This study found that organisations' websites share little information about their cybersecurity technology and strategies, and information regarding recent or historical cyber-attacks is even scarcer. The interviewed participants shared the same opinion and reported that they have found it difficult to learn from their peers when limited information is made available. Most participants felt this was detrimental to the industry and believe that collaboration with peers would help develop new innovations and new ways to approach their challenges. However, they also believed that industry and government should play their part.

Culture – There is limited existing literature on attacks on Australian organisations, and what exists generally comes from cloud-based cyber mitigation services (Akamai, 2020; NetScout, 2021b; Red Canary, 2021; Trend Micro, 2021). However, while not specifically aimed at cybersecurity-focused teams, there is literature regarding team dynamics, team performance, collaboration and how differing cultures, genders and diversity affect group outputs. According to the ABS (2022), technology is still heavily male dominated. Hofstede et al. (2010) discuss how countries with feminine cultures are more likely to develop solutions with a more inclusive outcome. This study's results support this view as it was found that many respondents did not want to talk about cybersecurity, even with anonymity, but as a percentage, female respondents were more likely to agree to be interviewed and share knowledge (see Figure 5.15, Section 5.5). Thus, does a participant's gender affect their willingness to collaborate and, if so, does this mean that leaders with these traits are more collaborative? This question opens the door to more research.

Diversity – This area covers more than the often-polarising male versus female arguments. Hofstede et al.'s (2010) framework takes a high-level viewpoint. The framework's six dimensions, which include the country's leadership style, the level of individualism and preference for long- or short-term orientation, could equally be used

to assess the attributes of groups and individuals. Individual behaviours are formed through a combination of inherent personality traits, education and experience, where education is delivered according to a country's national curriculum and experience is gained within the social structure of the country's culture. It is these behaviours that are used to assess threats and decide appropriate control actions. An organisation's cyber strategy can be based on the collective behaviours and learned knowledge of the team members engaged to develop it; therefore, differing groups will likely have a wide variety of solutions and objectives even when using the same technology to defend against a common opponent. This means that teams and organisations that are assembled from a more diverse pool of participants are likely to develop a wider range of potential solutions to choose from, and therefore diversity should not be limited to simply country of origin and gender. In fact, as the diversity term continues to grow and consider factors of age, race and religion, diversity could soon become too complex to describe. In Hofstede et al.'s (2010) six dimensions, the describing attributes are wide enough to be useful but remain simple enough to be practical.

Security – Within an organisation, once a strategy has been developed, controls and processes are constructed and circulated so that all operators follow the same methods when presented with a cyber event. When a cyber event occurs, following a process that was developed during a less stressful period leads to a higher probability that a favourable outcome will be achieved, which is similar to the processes used in emergency response planning (Foster, 2018). As an example, the Australian Government has recently mandated that its Essential Eight cybersecurity controls be implemented in the majority of federal departments and agencies (Hendry, 2021), although it is yet to be seen how each agency interprets the direction and how they may choose to implement the technology and process to comply.

Values – Having a process to follow is no guarantee that the outcome will be as intended. As opposed to computer-driven automation where processes are repeatable and have high consistency, processes that are carried out by humans can be influenced by the individual and their values. Schwartz's (2012) theory of values is similar to Maslow's lower levels of physiological needs and safety (Tanner & Raymond, 2012) in that it is held that all individuals have the same basic needs for food, water and

safety (Appendix D). However, according to Schwartz, they also possess 10 other needs that Schwarz divided into four groups, as shown in Figure 6.4.

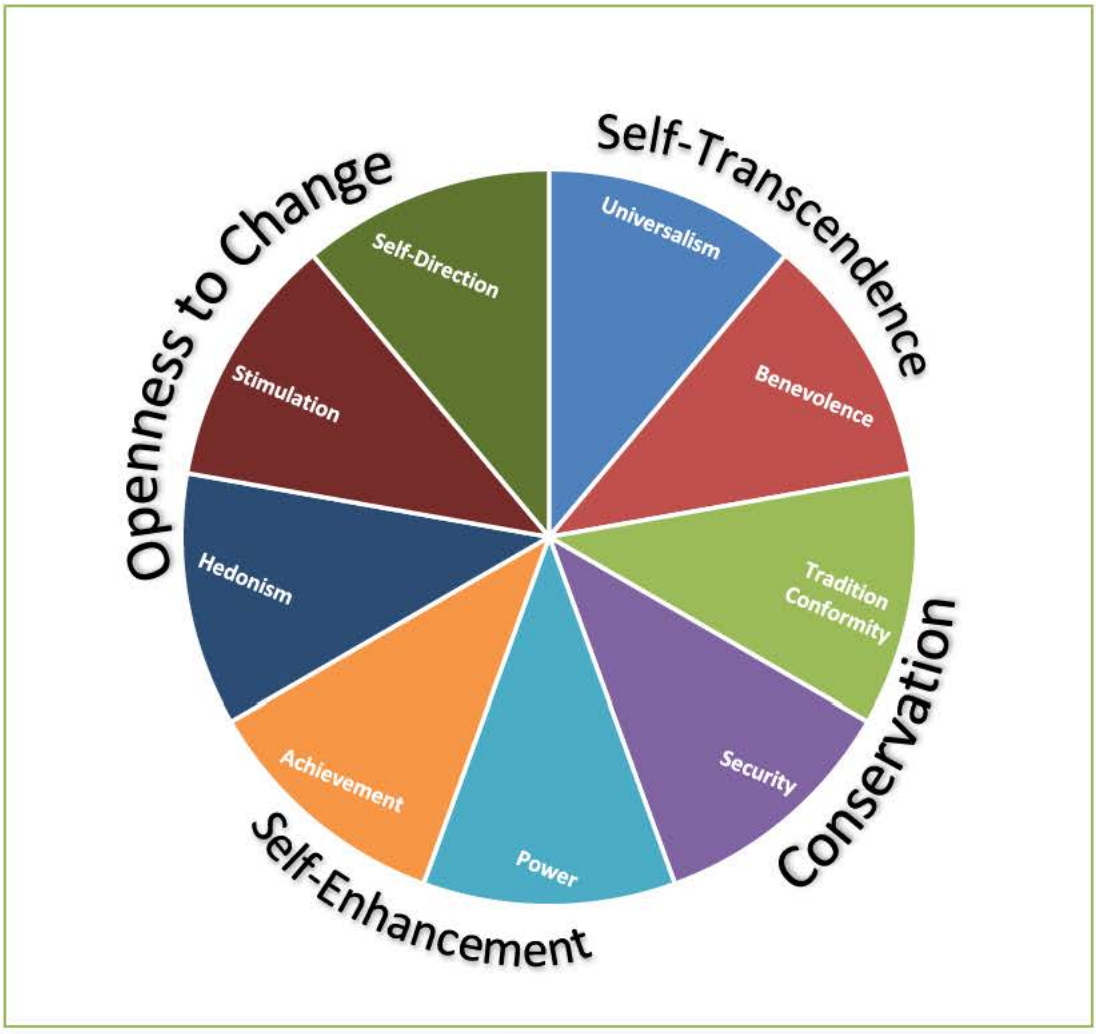


Figure 6.4. Schwartz's theory of values (adapted from Schwartz (2012))

In Figure 6.4, the two groups to the left include behaviours that focus on the individual such as achievement and hedonism, while collective needs such as conformity and security reside in the conservation and self-transcendence groups. Importantly, dominance for either collective or individualistic needs varies between different individuals and cultures. Those with a preference for collective values may seek to steer progress towards solutions that benefit wider communities, whereas those with individualist values may prioritise rapid remedies and personal success over a solutions inclusiveness (Hofstede et al., 2010). This means that the eventual outcome of an agreed process may still be affected by the individual's preferences and any

mistakes that they make while attempting to follow the process (including relying on memory or making assumptions that fall outside of their capability).

Human error – Human action is one of the key components that affect whether a cyber-attack fails or to what level it succeeds, and the reactive nature of the relationship between attacker and defender appears to amplify this factor (Henshel et al., 2015). The human factor is a well-known issue for cybersecurity professionals, and it forms one third of the people, process and technology triad (Herath & Rao, 2009). Human error can have extreme consequences and can render even the most comprehensive defences incapacitated (Reason, 2000). Also, as mentioned by several interviewees, any error or misconfiguration, deliberate or not, has the potential to have a significant effect on an organisation's reputation.

Human error could be classed as either intentional or accidental. Accidental errors can include typing errors in configurations, misunderstanding/misinterpretation of requirements or the simple exposure of credentials, such as a 'cut and paste' erroneously entered into an instant message channel. It is these types of errors that technology and process attempt to mitigate. The automation achieved with technology aims to ensure consistency through replication and an inability to deviate from command. It will deliver on instruction even if what is requested is incorrect, akin to garbage in–garbage out. Processes are built through experience and reactions to lessons learned, and they should be continually examined and improved in order to remain effective.

Intentional errors can be the result of aggrieved employees, espionage or social engineering. Aggrieved employees are those who work within the trust boundary of the organisation but wish to harm or inconvenience the organisation because of an event or perceived negative conditions. Depending on the level of access to systems, this could occur by direct manipulation of device configuration, deliberate exposure of confidential information to unauthorised recipients or alteration/destruction of data. These actions can be difficult to detect as the employees are often trusted and therefore likely to be under less observation than external activities. This attack method may be of greater concern as employees may have enough knowledge of systems to advise where attacks would best be placed and also have access to confidential or proprietary information, which any DDoS attacks that also seek to mask the theft of valuable data

would benefit from. In a similar way, espionage can make use of insider information gained through compromised employees. Espionage is again difficult to detect as protagonists attempt to keep a low profile and avoid detection (Grim et al., 2020). The difference between these two types is that the former is self-motivated and the latter motivated by competitors' or adversaries' reward. However, irrespective of the approach, the aim is to inflict damage, theft or disruption to the business and this espionage is undertaken to facilitate competitive advantage.

Social engineering can take many forms but relies on human interaction to be effective. Targeted methods such as phishing, spear phishing, smishing and vishing are aimed at deceiving the target and encouraging them to deviate from established processes to perform an action (Wang & Sun, 2021). They may use impersonation of individuals or devices to make their approach credible (Hatfield, 2018). Baiting and honeypots rely on an individual's curiosity, and a trojan-embedded web pop up or an infected USB drive left on a desk can be suitable opportunities for the curious to interact with and become the initial entry point of a cyber-attack. All these forms of social engineering could be considered an intentional act, as the employee's act of supplying information or access could be considered deliberate, regardless of whether the employee was coerced into supplying information or was left with little option other than to comply with the attacker's directions.

6.4.3.3 Governance, policy, communication and alignment

Organisations may understand the effect that differing individual motivations can have on their preferred approach and methods, so they may develop or rely on policies and systems of governance to ensure their desired outcomes are achieved and maintained. The following sections discuss how communication, governance and policy can impact alignment and how in combination, can influence end to end cyber defence capability.

Governance and policy – A high correlation exists between an organisation's IT governance and its IT business value (De Haes et al., 2019). As technology accounts for a significant portion of an organisation's expenses (Shimamoto, 2012), there is often closely related governance of IT budgets and operations. As a subset of this technology, cybersecurity may be even more sensitive and governance of cyber security efforts is vital for ensuring the optimal results of planning and investment are

achieved and for protecting customers, stakeholders, data and operations. Even the tightest and most well thought-out plans and processes may not achieve consistent results if the application of those plans and processes are loosely performed.

Organisational management puts information security policies in place and has the expectation that they will be followed by employees; thus, the policy's purpose is to ensure that employees meet expected standards, which is especially true when considering behavioural expectations, as human error is a key concern for organisations. Even if employees are willing to operate considerately without policies and the knowledge and experience to support them, the outcomes may vary (Da Veiga et al., 2007).

Governance in cybersecurity has the role of ensuring that plans and processes are implemented as intended, but the application of governance is also important as many plans and configurations are susceptible to cultural interpretation (Snowdon, 2015). Perception is an important part of how security decisions are made (Kearney & Kruger, 2016), and these individual perceptions are formed by mixing cultural and organisational experience with knowledge communicated by the organisation. This study found that most participants (20) reported a synchronicity of view between the organisation and themselves with respect to the perceived level of threat; however, while the participants were able to convey whether the organisation had changed its view over recent years, it is unclear from the results if their individual perceptions were their own or were heavily influenced by the organisation's posture.

Communication and alignment – According to Kearney and Kruger (2016), a lack of communication could lead to employees perceiving a gap in their organisation's information security program, especially when there is a lack of communication regarding risks or threats. This is especially meaningful as six participants commented that they were not aware of any cybersecurity plans. As all in an organisation should be supportive of the cybersecurity plan, not knowing the current threats and methods of mitigation could create gaps in the organisation's defences. Many outside of the technology department have direct contact with suppliers and customers, so while this directly impacts them due to any issues that occur, it also puts them at risk of attack due to their increased public exposure. Technology groups may benefit from security by obscurity; however, sales staff commonly publicly advertise parts of their

authentication credentials (email addresses, mobile phone numbers), which makes them more vulnerable. Without communication, non-technology staff could become the least informed but most vulnerable sectors of the organisation's workforce, which could be especially true around the time of an attack.

In the interviews, only four of the participants stated that a response to an attack would include a wide array of organisational staff. Most responded that a specific group would communicate with close collaborators, with technical staff being the most popular choice (16). Notably, stakeholder management was only mentioned by two respondents, which aligns with the findings from the website analysis, which found little is published by organisations on their cybersecurity technology and events. This could potentially be by design, as the organisation may seek to protect its reputation until a positive message can be published. Alternatively, as the focus during and post attack is reported to be aimed at technical remediation works, any lack of public and stakeholder notification may simply be an omission. However, in one case, government notification was a licence requirement and stakeholder notification was therefore stated as a high priority.

Governance in organisations is there to ensure policies are adhered to and processes are followed irrespective of the stress and pressure that cyber events can create. However, stakeholder notification was only included when government legislation demanded its inclusion; therefore, cybersecurity governance enforced from an Australian Government level appears to have a practical effect. As individual knowledge and experience influence personal threat perceptions, greater exposure to cyber-attacks could foster greater awareness of cybersecurity vulnerabilities.

At its higher level of authority in Australia, the government has a role to play in developing Australia's cybersecurity capabilities. As mentioned in the literature review, other countries invest significantly in cyber capabilities, with Israel being one of the highest investors recorded. While the Australian Government has invoked plans to raise awareness, and in some cases have offered grants to SMEs to help raise cybersecurity standards within businesses, they have fallen short of the investment provided by other governments. Therefore, while countries such as Israel heavily invest in the cybersecurity training and education of its population, Australia's investment is much smaller. For example, the comparably smaller cooperative

research centre (CRC) program involves only 10% of Australia's 38 universities (Cyber Security CRC, 2021). One member of the CRC is the ASD, which developed the Essential Eight in 2010 (ACSC, 2021). Recently, as part of their defence policy through the Attorney-General's Department (AGD), the Australian Government have imposed a direction through an amendment to the Protective Security Policy Framework (PSPF) for all non-corporate commonwealth entities (NCCE) to fully adopt its mitigation strategies (Anderson, 2021). However, this recommendation only covers NCCEs and does not extend to private or other public entities, so the government is essentially looking after its own backyard.

In the interviews, the participants suggested that the government had a role to play in cyber defence. The wider introduction of policies such as these could help raise Australia's overall defensive capability. As a chain is only as strong as its weakest link, so too is Australia's cyber defence only as strong as its weakest entry point. Raising the level of defence across the board may help to deter 'supply chain attacks' where bad actors attempt to infiltrate vendors and smaller, less-protected organisations as a stepping stone to their larger intended target.

6.4.4 Motivation and COVID-19

Drivers for change can arise from proactive ideas, such as the desire to improve the capabilities or performance of a product, or reactive response, such as when products are found to be harmful during testing or customer use. While proactive motivations can provide a more relaxed atmosphere to plan, reactive changes still require thoughtful consideration, and both drivers can be susceptible to the pressures of developing new solutions to presented challenges.

Outbreak – In December 2019 the world was forced to respond to a new threat that had the potential to infect the global population. The COVID-19 outbreak impacted on the world, and this biological virus was serious enough for governments to invoke radical plans and policies to slow or stop its progression (Johnston, 2020). These new policies had a significant effect on society. Whereas societies have previously come together to endure a crisis, this pandemic forced the opposite. Mask wearing became mandatory, public entertainment was either cancelled or postponed and there were unpopular restrictions on group sizes in public and private and in indoor and outdoor venues. These restrictions created difficulties for businesses, as those with more staff

than could legally gather in an office area were forced to quickly adopt new ways of working remotely, which required an increase in the use of virtual communications systems and modification of organisational practices, without which meeting new social distancing requirements would prove impossible.

Reactively Remote Working – With this sudden shift to remote working came an increase in the threat of cyber-crime, as the opportunities for criminal activity shifted from physical to online environments. In addition, the sudden rush by organisations to respond to the pandemic crisis meant that technology teams were focusing on crisis management rather than planning this adaption to a new way of working, which meant that the move to remote working occurred with much less planning than ordinarily permitted and helped to create more cybersecurity gaps in the organisation's defences (Miller, 2020; Skilijic, 2020). Employees were rapidly forced to work from home with little consideration of the security complications of passing (in part) cybersecurity governance to the homeowner (Abukari & Bankas, 2020; Miller, 2020; Wirth, 2020). As Chapman (2020) states, working from home can attract similar challenges to bring your own device (BYOD). As with BYOD, personal devices used for work in the home should, at a minimum, be secured with levels of anti-virus software and password protection that align with company policy (Chapman, 2020). Furthermore, the method of connectivity needs to be considered, with options such as reliance on the homeowner's ISP, the organisation's VPN or authentication aligned with a zero-trust model.

Governance – COVID-19 led to more staff working from home for extended periods in a less formal atmosphere. When entering a business premises, staff are encouraged to adopt the cybersecurity standards of the organisation either through training, awareness programs or simply through osmosis. However, at their home, there are many more distractions that may result in an employee making critical mistakes or errors in judgement (Irwin, 2021). For example, they may apply less scrutiny or caution when clicking links in emails or assume that the poor performance of a system is due to home-grade networks, which may lead to accepting the issue rather than reporting it. Research by (Johnston et al., 2010) supports this. In their study of 500 remote and office-based employees, they found several factors that influenced information security policy compliance between the two groups and noted differences

in perceived levels of security and privacy policy awareness, self-efficacy and compliance intentions. They suggested that these differences may be due to the reduction in the available support for encouraging remote workers to adopt security and privacy policies. As a result, home cybersecurity practices become misaligned with those of the office, which undermines employees' ability to comply with the organisation's security posture (Johnston et al., 2010).

This lack of compliance may be one factor that increases the risk of (often unintentional) insider threats, as a report by CYBSafe stated that a third of the UK's SMEs surveyed had experienced a cyber-attack as a direct result of an employee working remotely (CYBSafe, 2018), and a later report showed that in 2020, 90% of their surveyed SMEs concluded human error to be the cause of their data breeches (Goodman, 2020).

Catalyst for growth – Cybersecurity threats appear to have increased during the COVID-19 pandemic, and the methods used in the attacks have adjusted to the new ways of working, with many organisations reporting an increase in malicious websites, malware, spyware, ransomware and DDoS (Khan et al., 2020). COVID-19 has also been used as a tool, as attackers have turned to using fake COVID-19 information sites, mobile apps and email scams (Khan et al., 2020). As staff are working in isolation, confirming the legitimacy of the many requests received becomes a task that requires additional effort, which can be a task that fails to be actioned without the support normally provided in the workplace. This is important, as social engineering attacks account for just under 40% of all cybersecurity attacks, with approximately 38% of these attacks being attributed to phishing (Bassett et al., 2021). As cyber criminals often use some form of social engineering to gain intelligence or credentials (J. P. Morgan, 2021) that can be used directly against the victim or indirectly against associated targets (e.g., impersonation, blackmail, DDoS, etc.) (Bermudez Villalva et al., 2018), methods that can reduce the success of these type of attack could be beneficial.

Defence – Preventing the success of attacks is vital as individuals are more likely to respond to the effects of a cyber-attack than the attack itself. For example, when a cyber-attack targeted Ukraine's power grid in December 2015, in which 230,000 residents were left without power (Zetter, 2016), the public (demonstrating Maslow's

hierarchy of needs) were more concerned with the lack of power, heating and ability to prepare food than any malware introduced into the power control centre's systems. In a similar way, staff working from home may be more likely to be concerned with the impact of the attack than reacting to any early signs of cyber-disruption, and may only act when the outcome begins to inconvenience them or indicates the possibility of imminent consequences. This course of action is potentially a behaviour that is shaped by media coverage, as media headlines focus on the dramatic outcome and only provide information on the cause of the attack later in the report. This method of reporting aids extortion by motivated cyber criminals who wish to distribute propaganda and rely on the media to raise awareness of the impacts their attacks produce, which is similar to the strategies of terrorists (Minei & Matusitz, 2011).

Security posture – The effect of the pandemic has highlighted a need to find ways to extend a business's cybersecurity posture to the home and maintain its efficacy. This could be achieved through greater effort with awareness programs, but awareness itself does not guarantee behavioural change (Bada et al., 2019; Ertan et al., 2020). Greater success may be achieved through the development of cybersecurity knowledge and awareness in the workplace in such a way that it can easily be extended to the home environment (Alshaikh & Adamson, 2021). One way to deliver this could be to develop an individual-based security culture that endures irrespective of whether the employee is workplace based or a remote worker. To be effective, this individual approach may rely on the ties formed through the psychological contract that exists between an organisation and its employees. These implicit agreements that align individual and organisational beliefs and cover the implied terms of exchange may help to maintain trust during periods of transformational change, and successful change may improve cybersecurity awareness, adherence to the cybersecurity posture and the stability of employee satisfaction and wellbeing (Rousseau, 1996).

6.5 Main Findings

The eight new findings reached in this study are listed in the table below. These findings add new areas of knowledge to six of the seven macro themes discussed in this research and are briefly explained in this section. More detailed discussion can be

found in the previous section (Section 6.4) and in the following section (Section 6.6) where the implications of this new knowledge are discussed.

Table 6.10

Main Findings Related to Macro Themes

Finding Number	Macro theme	Micro theme	Response or source of finding
1	Approach	People	The importance of diversity
2	Communication	Collaboration	Experience sharing and cybersecurity events database
3	Communication	Collaboration and reliance	Lack of organisational transparency
4	Method	Reliance and capability	Reliance on internal capability and reactive plans create narrow expertise
5	Method	Collaboration and governance	Minimum standards
6	Motivation	Communication and collaboration	Leverage
*	Risk ownership	No new knowledge	
7	Risk	Data and reputational loss	Chief concerns
8	Threat	DDoS	What is important to businesses

6.5.1 Approach

Finding 1

The academic literature reviewed in this study covered at a high level how DDoS and other cyber-attacks may be used by a range of actors and the potential motivations for these attacks. Much of the practitioner literature was written by vendors, and it focused on the methods and technology organisations might use to mitigate the various forms of DDoS attack, but this information was written from a perspective that sat outside of the organisation. With the demonstrated lack of transparency related to cybersecurity found in organisations, it is difficult to understand how accurate these perspectives could be, and it is likely their recommendations are presented as a "cookie cutter" type solution. This study found that organisations mostly prefer to manage their defence strategies using internal capabilities, but participants felt that while they

currently have enough knowledge and experience to perform their role, gaining additional skills and diversifying their perspectives would enhance their capabilities. As such, organisations who have a gender bias in their staff may be failing to exploit the benefits of a diverse workforce but due to the current organisational discomfort with sharing, knowledge is likely to remain inside organisational boundaries.

6.5.2 Communication

Through information sharing, greater understanding and alignment can be achieved. Commonly, organisations often protect information from external access but share information between teams. However, this study found this is not always the case. Communication, both internal and external, are important factors that support the delivery of an effective cyber security strategy and this research found where employees felt more effort should be placed to alleviate this potential deficiency.

Finding 2

Organisations appear to have a preference to retain knowledge and experience inside their company boundaries and share very little with anyone external, even when specialist companies exist to provide specific subject-matter expertise that may benefit them. This includes mandatory reporting as well as voluntary collaboration. While some organisations are required to report cyber-attacks such as data breaches (OAIC, 2021b), there is no publicly assessable register of these attacks available in Australia. As such, most public awareness is directed at attacks that affect a large or critical operation (such as the Colonial Pipeline attack) (Metcalf, 2020). Many smaller attacks on less well-known companies go unnoticed or unreported, but the information from these could be more relevant to many more similar-sized and similarly operating organisations. A requirement to report may be one way to generate a central pool of knowledge from lessons learned and provide a resource that could help raise the capability of Australia's industry as a whole. Irrespective of this option, participants expressed their desire for greater collaboration and would welcome a forum for this to occur.

Finding 3

External communication is not the only area to experience difficulties. Several participants raised the issue of a lack of transparency around cybersecurity within their organisation, with one stating that those that operated the cybersecurity role

deliberately acted in obscurity. This is a surprising finding as the human factor is acknowledged by both the academic and practitioner literature as being an important issue for cybersecurity, and deliberately restricting this type of knowledge seems counter intuitive. One possibility is that there is limited knowledge in the organisation, as some participants stated that the responsibility to defend sat with their vendor for cybersecurity. However, this maybe an inaccurate impression as some cybersecurity ownership remains with the client. AWS make it clear in their product statements where they believe responsibility sits:

> *AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services* (AWS, 2022, para. 2).
>
> *Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks* (AWS, 2022, para. 3).

However, many organisations employ cybersecurity awareness programs to combat the vulnerabilities incurred from awareness deficiencies, but this study's findings show that there may still be room for improvement in this area.

6.5.3 Method

When implementing cybersecurity defence, the method organisations chose may be influenced by the source of motivation for change. Those in roles with wider visibility may observe different priorities than those with access to finer grained details and as such, top-down direction may differ to bottom-up requests, even within the same organisation, experiencing the same challenges. As such, some areas, such as data loss prevention, may be considered as a greater priority than loss of service, and this may lead to some areas of cyber security being disregarded for consideration. Frameworks seek to cover this by applying a standard view across all organisations and this

standardised viewpoint ensures unimportant areas are at least considered and documented, even if ultimately discounted.

Finding 4

An organisation's preference for internal capability reliance extended to their lack of use of established cybersecurity frameworks. Those that had been attacked preferred to develop their own defence strategy, which may have some advantage in certain circumstances. With the lack of knowledge sharing between organisations, companies who had recently been attacked could have superior, fresh and up-to-date knowledge attached to raw experience that may enhance their capability as they develop their defences, but their enhanced capability may be limited to the narrow attack vector they recently experienced. Those that had just been attacked may also have been under some pressure to quickly develop and implement a solution, which may explain the lack of use of established standards as these can take time to apply. However, of the participants in those companies that acted proactively and had more time to develop their strategy, very few mentioned the use of frameworks, which raises further questions. The guidance of established frameworks combined with capability and experience may produce an optimal result; therefore, if frameworks have been carefully developed over time, why are organisations not using them? Do organisations know they exist, are they inaccessible, are they too complex, or should there be something simpler?

Finding 5

As use of the internet moves towards becoming a basic need (Xie et al., 2020), abstinence becomes increasingly difficult. As such, participants raised one opportunity to help raise the base level of cybersecurity defence in Australia. They commented that the introduction of minimum cybersecurity standards for connectable products sold in Australia would improve baseline defence capabilities. As cybersecurity experts make up only a small proportion of the Australia workforce, it likely that this is also reflected in the population as a whole, so this idea would certainly help the majority of Australians who lack sufficient cybersecurity knowledge to implement new devices with optimal security configurations.

Finding 6

To implement a cybersecurity plan, organisations require motivation, and where this motivation is derived from influences the types of challenges that will need to be overcome. This motivation can be provided by leadership teams passing direction to technical teams to create or modify existing solutions in response to new ideas and strategies developed by leadership. In other cases, it may be the technical teams who identify vulnerabilities that need to be addressed. However, in both cases, communication and negotiation need to occur for the plan to be implemented successfully. Without good communication, technical teams may not implement solutions exactly as leadership teams expect, and where ideas are formed by technical teams, they may not be able to convince decision makers to approve their projects. This supports the need for greater collaborative effort so that the technical teams can have more understanding of the strategic needs of their leadership teams. Similarly, with more experience, decision makers may more easily appreciate the risks presented by technical teams in their proposals. For example, as loss of data is a common occurrence, backup proposals are easily understood, but the same cannot be said for cybersecurity risks that have yet to be witnessed in the organisation.

Finding 7

Of the participants, 25 considered DDoS to be a real risk to their organisation and their organisations had included mitigation for DDoS in their cybersecurity defences, with 57% implementing a specific mitigation inside that plan. However, participants reported that there was more concern with the loss of sensitive information such as PII, PCI and PHI and the reputational damage that exposing these may incur. As such, they tended to focus on any type of cyber-attack that could facilitate that outcome, and those whose business had less reliance on technology paid much less attention to these risks.

Finding 8

The practitioner literature discussed the threat created by IoT devices and the risks for physically remote infrastructure control systems, and participants were more concerned with the loss of property over the loss of service. Most participants commented on the risk of loss of data, intellectual property and sensitive information and how this could impact on future business. Participants were also concerned with

loss of service or network connectivity but they viewed this as less of a risk than property loss, maybe because victims of DDoS are inconvenienced for relatively short periods whereas loss of intellectual property can be an indefinite loss. However, a DDoS could have a major effect if timed with periods of critical network use. Hospitals, for example, require stable connectivity for the transfer of critical and timely patient information, and in other sectors such as the gambling entertainment industry, organisations may suffer losses if a DDoS prevented network access during an important sporting event.

6.6 Implications

The implications of the findings reached in this study have been addressed through five categories: practical, policy, social, theoretical, and methodological.

1. The implications for practice are the identification of new knowledge that may be useful to adopters of technology and information on the potential challenges they may face as they attempt to use a secure approach when implementing new systems and services. The practical implications also connect with policy, as practical applications often need to fall within policy guidelines.
2. The implications for policy are the highlighting of areas where current policies may be deficient and providing an insight into what participants believed would support the delivery of a more secure internet for Australia.
3. The social implications are the effect this new knowledge could have on society. The study identified how greater understanding of the motivations of individuals and their need for more knowledge and collaboration may help organisations implement strategies that more closely align with their staff needs. The findings also demonstrate how actions with smaller social groups such as teams, departments and organisations can affect the larger social circles of industry and country.
4. There are theoretical implications for the theories relating to human motivation and technology development. The findings of the study provide a greater understanding in knowledge in this area and suggestions for the application of new standards that could enhance Australia’s cybersecurity posture overall.

5. The implications for the methodology result from highlighting where challenges in the research process have occurred and identifying how this may have impacted on the study so that future researchers may plan to avoid similar difficulties and benefit from knowledge of successful methodological strategies.

6.6.1 Practical

Combining the comprehensive academic and practitioner reviews with website analysis and semi-structured interviews, this study's findings add to the pool of existing knowledge of how organisations consider the threat of DDoS within a cybersecurity context. One significant contribution from the study's findings is the identification of organisations' preference to develop their cybersecurity strategies in isolation, which is in contrast to the academic literature suggesting that greater capability can be achieved through diverse cultural collaboration (Hofstede et al., 2010; Kolenko, 2019) and the practitioner literature promoting the use of formal frameworks and specialist external assistance (ACSC, 2021; Chipeta, 2021). In cases where the organisation specialises in cybersecurity or where the organisation has recently been the victim of an attack, their capability level may exceed that of others, but for the vast majority of organisations, failure to absorb and utilise existing knowledge and expertise may lead to a suboptimal result. Recognition of this deficient strategy may result in an organisation adopting a more collaborative path.

This lack of willingness to collaborate was also manifested in a lack of communication and transparency within organisations. Cybersecurity is everyone's business (Brisson & Savoie, 2018), which is a view supported by the many awareness programs implemented by organisations. However, the findings reveal that organisations do not always share their cybersecurity strategies with their staff, which can bring about a potential deficiency, as without guidance or knowledge to encourage alignment employees may choose to implement security using their own culturally inspired perceptions (Kolenko, 2019). While these choices may be good in isolation, they may not integrate well with organisational policy. Further, this detrimental effect may be amplified in periods of mass remote working as there is little immediate peer support to encourage organisationally preferred paths of action when face-to-face contact is scarce.

This lack of communication is further surprising as many participants expressed their desire for more training and the chance to gain knowledge from other organisations who have first-hand experience. Gaining access to first-hand experience rather than secondary sources or the experiences of others that are written through the lens of an author may bring greater insight and a broader perspective to the learning experience.

While this may be an appropriate direction for those with technology knowledge, pursuing this type of training and experience sharing may not be suitable for those who are less comfortable with technology. Participants' thoughts on minimum standards for technology products sold and implemented in Australia may fill this gap in Australian defence. Consumers have the right to expect that the products they purchase are safe to use and perform as described (Australian Consumer Law, 2016), and the participants thought this view should be extended to the default level of cybersecurity included and configured in connectivity-capable products. However, the method of configuration of these products should be simplistic so that less technically knowledgeable consumers can still configure devices in an optimally secure way; for example, automating configurations using AI and ML to configure the device based on analytics (Cisco, 2020). Securing these products brings advantages in two ways. While consumers who purchase these products should gain increased protection of their assets, being able to protect these devices from being compromised and used as resources for attacks on others (e.g., the Mirai botnet (Woolf, 2016)) should help reduce the likelihood of future large-scale DDoS attacks.

6.6.2 Policy

There are two areas of implication for policy evident in this study's findings. First, while the introduction of minimum cybersecurity standards appears to have positive practical value, the mere introduction of these without competent governance would rely on significant consumer pressure to ensure its success. Currently, without enforcement, manufacturers seem to only add security options when driven by market demand (Blythe et al., 2020; Paul, 2020). The recent raised visibility of cyber risks (Paul, 2020) may have influenced consumer choice, but consumers still have the choice of purchasing less secure or insecure alternatives, and those consumers without knowledge of technology may not fully understand the difference in security level between products (Blythe et al., 2020) and may not consider security as highly as other

deciding factors. For this reason, the participants recommended the introduction of governance and legislation to enforce a minimum standard.

Second, as this study proceeded, it found that Australia does not have a publicly assessable cyber-attack register. Australia does have a requirement to report data breaches to the OAIC, but this is only required in limited circumstances (OAIC, 2021b). From these reports the OAIC does provide statistics, but again these are limited, de-identified and without the level of detail cybersecurity practitioners may prefer. Participants expressed their desire for a greater sharing of knowledge; however, these statistical reports are probably of little use to those seeking to gain further understanding as they seek to improve their methods of detection and management of cyber events. Some information is provided by independents (Center for Strategic and International Studies, 2022; Kost, 2022; Webber Insurance Services, 2022), but this is often limited to attacks on well-known organisations and relies on third-party published reports rather than direct knowledge provided by the victim. A national database of cyber-attacks similar to the Repository of Industrial Security Incidents (RISI, 2015) could be a useful way to disseminate practical information to cybersecurity professionals. However, to populate a database of this type may require more extensive coverage in the policies that direct cyber event reporting obligations.

6.6.3 Social

Organisations face a constant and difficult challenge to defend themselves against cyber-attacks (Fielder et al., 2016) and with limited collaboration they can be limited to the strategies they have available to address their cybersecurity vulnerabilities. Therefore, a potential social change that may result from this research could be greater understanding of workforce needs, along with insight into employees' internal drivers to maintain safe and secure access to the systems and data they are custodians for. Also, through increased awareness and application of new knowledge gained from this study, future developments in Australia's cybersecurity strategies may more widely support elements of the UN's SDGs.

SDG Goal 6 - Clean water and sanitation

The UN's sixth goal, "clean water and sanitation" seeks to ensure the availability and sustainable management of water and sanitation for all (UN, 2022a) but Vitek Boden

proved that water treatment can be vulnerable to attack (Sayfayn & Madnick, 2017). This vulnerability results from the infrastructure control systems historically being closed loop hardware programmable logic controller (PLC) systems that required close proximity for human interaction to occur. As such, their design focused on functionality rather than security, as the security could be applied physically. More recently, the use of supervisory control and data acquisition (SCADA) systems that operate as a software platform open up access to remote workers and the ability to connect via WANs or VPNs. While Boden bypassed physical barriers to inflict his sewage attack, the increasingly available connectivity means that vital areas of infrastructure such as water have a greater threat landscape to consider. This study's finding shows that greater collaboration and greater transparency with regard to previous attacks can have benefit. In this case, water treatment providers have already benefited from the experience of the Maroochy Council, and this study's finding show this is a strategy that should continue.

SDG Goal 9 - Industry, innovation and infrastructure

The threat to infrastructure is not limited to water treatment plants, as all infrastructure is now potentially vulnerable. As discussed in the literature review, the Stuxnet attack of 2010 (Fruhlinger, 2017) showed the possibility for using software to attack infrastructure and its ability to deliver damage to physical devices, which is relevant to the UN's ninth goal that aims to "promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all" (UN, 2022a). As such, the findings of this study are important to all industries and are not limited to collaboration and knowledge sharing between industries. This study's findings regarding communication are relevant as greater intra-company transparency and communication would help all employees to become more vigilant and help them not just to identify anomalies but also have greater awareness of processes to report them, which would improve defence capabilities as a whole.

SDG Goal 11 - Sustainable cities and communities

Although the human factor is a major consideration for cyber-security, humans act with technology, and it can be a deficiency in technology that creates a vulnerability. As seen with the Mirai botnet attack during 2016, vast quantities of insecure devices were combined and used as a resource to attack a critical component of the internet

(DYN DNS) (Woolf, 2016). This appears to contradict the UN's eleventh goal, "make cities and human settlements inclusive, safe, resilient and sustainable" (UN, 2022a). Australia's desire to pursue the smart city movement could increase their vulnerability to attacks of this type if insecure IoT devices are implemented en masse. IoT is an important part of the strategic plan to increase the efficient use of city resources, but rapid IoT development can be focused on functionality with insufficient attention to security. For example, a recent trial of pedestrian tracking was conducted around Macquarie University where there were 74 sensor nodes installed. This IoT trial used Arduino UNO as the processor and the data were uploaded to a server via LoRaWAN (Akhter, Khadivizand, Siddiquei, Alahi, & Mukhopadhyay, 2019); however, there was no mention of cyber-security in this article. This is worrying, as the Arduino as a development microprocessor is known to have vulnerabilities if not configured appropriately (Gendreau, 2016), and although LoRaWAN is thought to be secure, it can also be vulnerable in some circumstances (Dudek, 2021). This supports the studies finding that there is benefit in the implementation of legislated minimum cybersecurity standards for networkable products, and that this benefit should be combined with governance to ensure adherence.

SDG Goal 8 - Decent work and economic growth

The ACSC, which is a statutory agency and part of the ASD, recently reported that they received 67,500 cybercrime reports in the 2020–2021 period, a rise of 13% over the previous financial year. They also reported that self-reported losses from cybercrime totalled more than $33 billion. These figures contradict the UN's eighth goal, to "promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all" (UN, 2022a). The Australian Government estimated its total revenue as $472.4 billion for the same period (Hawkins, 2020), so the loss to cybercrime is not inconsequential.

The findings from this study found that participants' greatest concern was the loss of data and reputational damage, which aligns with the ACSC report, and this study thus provides organisations with insights into how employees could gain increased capability. It also provides other visions that could be implemented to reduce organisations' threat landscape. Application of these may become a catalyst for change that may lead to greater outcomes from cybersecurity strategies.

SDG Goal 17 - Partnership for the goals

Finally, the UN's seventeenth goal, to "strengthen the means of implementation and revitalize the global partnership for sustainable development" (UN, 2022a) has a related goal that is specific to technology. The UN (2022b) states that "technology, science and capacity building are major pillars of the Means of Implementation of the Post-2015 Agenda" (UN, 2022b, para. 4). Therefore, future technology implementations should be performed using environmentally responsible technologies. These studies findings are in line with that aim, as the findings support the reduction of cyber vulnerabilities and a focus on more effective cyber defence practices.

6.6.4 Theoretical

Cybercrime is a complex subject as it includes aspects of both a physical (technical) nature and the human side of motivation (attack and defence). Therefore, it has not been possible to provide an all-encompassing theory but instead, theories have been borrowed and applied where suitable. From a human perspective, four theories were used to understand more of the human reaction to threat and their motivation for action. Maslow's hierarchy of needs (Tanner & Raymond, 2012) and McClelland's trio of needs (McClelland, 2010) were used to understand the human internal drivers, and Hofstede's cultural dimensions theory (Hofstede et al., 2010) was used to show that these internal values can be influenced by cultural upbringing. Roger's (1983) protection motivation theory added a reactionary perspective to this as the theory examines how humans react to perceived threats; however, this reaction may be influenced by internal needs and the values adopted through cultural upbringing. Bringing these theories together appears to be a good solution as the need to view from different perspectives remains a necessary progression.

Three theories were used to investigate DDoS on a more technical level: Moore's Law, which theorised that the density of transistors in an integrated circuit (and hence computing power) would double every two years (Moore, 1965), Kryder's Law, which considered how the density of physical storage could increase in relation to computing power (Walter, 2005), and Koomey's Law, which focuses on computing power consumption (Koomey et al., 2011). Of these, only Moore's and Koomey's laws appeared to be aligned, as Kryder's law slowed when storage devices switched to solid

state media. Both Moore's and Koomey's laws showed exponential growth (Figure 2.1 and Figure 2.2), and this growth curve was similar to the growth curves of internet adoption (Figure 2.7) and volumetric DDoS records (Figure 2.3). But how much is too much? For reference, the volumetric DDoS record currently sits at 2.7 Tbps (Nicholson, 2020), which is slightly more than Tasmania had in 2017 via two Telstra subsea cables (Bass-Strait-1 and Bass-Strait-2) at 1 Tbps each (Telstra, 2017).

The implications of these findings are that expectations are being realised, as the growth of processing power and greater internet adoption are fuelling the resources and targets that enable DDoS to occur. As growth is also likely to continue as more IoT devices are introduced, this study's findings regarding the importance of minimum standards for network devices shows great relevance for the future.

6.6.5 Methodological

This study followed an exploratory research path as the initial research and literature reviews found very little on the subject matter. Further to this, website analysis yielded little depth of information, which led to the choice of semi-structured interviews with organisational staff. However, this also was not without challenge. This study was undertaken during the COVID-19 pandemic, and this had some effects on the cybersecurity landscape and the process of the study itself. During the pandemic, many staff needed to work from home, and this placed a great load on organisations' remote infrastructure. In many cases, urgency was focused on a rapid workable solution with security a second consideration. For example, while company-owned laptops may have policy-driven security configurations, little to no audit would be performed on the home-based infrastructure to which it was connected. Therefore, COVID-19 rapidly changed the field of study and may have influenced the thoughts of the interview participants. It may have also influenced their willingness to participate. In addition, the interview process needed to adjust. Without the ability to perform face-to-face interviews, videoconferencing was used, which altered the dynamic of the planned semi-structured conversations. Observations of the protection motivation theory in use (Rogers, 1983) may be more visible in the home environment, as the isolated environment is less diluted by organisational interference and influence, and this may be a future research direction. The analysis of interviews was primarily qualitative with additional demographic information, whereas the website analysis

used quantitative methods and descriptive analysis; however, with more direction, future studies could utilise mixed methods.

One limitation of this study was the size of the pool of participants. Future studies should be aware of the difficulty in recruiting participants and should discover preferable methods to connect with willing participants so that future studies can consider greater depth and breadth of input. A second limitation was the number of industry sectors covered. The ABS (2020) detailed 18 industry sectors and the study participants came from approximately half of those. Future studies may wish to incorporate more sectors to see if the themes raised in this study continue throughout all Australian industry sectors. However, despite this limitation, exploring how organisations view DDoS as part of their cyber defence strategy was an important subject for research. Performing this research during the COVID-19 pandemic added another characteristic. While it created some challenges to the research process and delivery, it also provided a unique opportunity to perform this type of research in an uncommon social situation.

6.7 Summary

This chapter began with the identification of macro (Section 6.2) and micro (Section 6.3) thematic categories that were then collated into four groups (Section 6.4). This helped guide the discussion as it was linked to the knowledge gained from the combined literature reviews. The first group, threat, risk and risk ownership, examined participants' thoughts on threat and formed comparisons between the methods companies use to assess general risk compared to how they assess the risk of cyber-attacks while acknowledging the similar methods of mitigation. Approach, method and technology, the focus of the second group, considered the four different approaches to risk management of risk based, maturity based, reactive based and transference before discussing the methods used, including using the organisation's own experience, using guiding frameworks or using a combination of both. Also addressed was the role of technology, specifically the lack of standards for products and configuration methods. The third group discussed capability and communication, highlighting the prevalence of academic and professional cybersecurity qualifications and the preferences seen in advertised roles. The final group, motivation and COVID-

19 examined participants' and organisations' motivations to address DDoS and how COVID-19 brought an additional factor to consider.

Section 6.5 discussed the eight main findings of the study in relation to the seven identified macro themes. These findings included how organisations approach their cybersecurity strategy, such as their preference to retain knowledge and base their strategy on their own their experience rather than share experience and further improve, how gender bias in industry may impact on the benefits a diverse workforce can bring and the cyber risk participants were most concerned with. Finally, in Section 6.6, the implications of these new findings were addressed through five categories (practical, policy, social, theoretical and methodological).

Chapter 7: Conclusions

7.1 Conclusions

The work in this thesis has shown that distributed denial of service (DDoS) can be complex, but is an easily accessible form of cyber-attack with a very low barrier to entry. Since its inception in 1974, it has grown from a small annoyance used by computer hackers to win "king of the hill" battles (Radware, 2017) to a credible international threat used by activists, criminals and countries to achieve their goals (Nicholson, 2022). The scale of attack has grown from the small beginnings of a few networked computers to hundreds of thousands of devices combined to produce attacks of up to 2.3 Tbps as seen in the attack on Amazon Web Services (AWS) in 2020 (Nicholson, 2020). To put that scale in perspective, most home internet connections in Australia are lower than 100 Mbps (Optus, 2022; Telstra, 2022). Business internet connections may reach 10 or 1000 times that, but even a link providing 100 Gbps bandwidth would be overwhelmed many times over during an AWS scale attack.

As I performed my literature review, I gained knowledge from practitioner sources that showed that the ability to scale is not the only threat. Sophisticated methods could allow smaller requests to have great impact through reflection methods, such as those that use Network Time Protocol (NTP), which can have a 1:200 request to response ratio. Other attacks that seek to overwhelm weak points in infrastructure, such as an HTTP Flood (Technology Org, 2018), may be equally difficult to detect before the impact is experienced. According to the practitioner literature, DDoS is a current and valid threat. However, while the practitioner literature carries much information on the history of DDoS, methods of mitigation and observational analysis of high-profile attacks (Ghoshal, 2018; Nicholson, 2020; Woolf, 2016), in general, they discuss technical difficulties but fail to cover the experiences of the victim organisations themselves or the thoughts and feeling of the employees within.

The review of the academic literature also failed to reveal these perspectives. The academic literature provided good information on potential and theoretical methods of

motivation, as well as observation of what influence a country's GDP per capita, military size, freedom of speech and culture (Hofstede et al., 2010) may have on proactive and reactive actions, and how decisions regarding cybersecurity are made. The academic literature also showed how a country's strategy could improve their cybersecurity capabilities (Cohen, 2018), how organisations should consider their employees' attitudes to cybersecurity (Foltz, 2004), and how, as individuals, our needs and drivers may influence our approach to problem solving (Huang et al., 2010; McClelland, 2010; Tanner & Raymond, 2012). However, while the reviewed sources provided deep and contextually relevant information, they did not cover the perspectives of employees in organisations, and hence this research aimed to fill this identified gap in knowledge.

After reviewing several potential paradigms and research methodologies, interpretivism and a combination of exploratory and descriptive research were determined to be the best fit for the study. The use of semi-structured interviews and the adoption of an interpretivist perspective allowed me to acknowledge my potential influence and bias as I performed the data analysis. The exploratory research method allowed me some freedom to explore and uncover initial areas of interest as I formed the assumptions, limitations and research questions that ultimately guided this research project. Without this exploratory research, it would have been difficult to conceive useful parameters, and the established assumptions and limitations were continually adjusted as understanding became clearer. For example, my assumption that employees would be comfortable with providing their opinions on DDoS when guaranteed anonymity proved to be inaccurate. This inaccuracy required reconsideration of the limitations, which in turn affected ethics approval, the scope and the duration of data collection. The exploratory research catered for these unknowns through its inherent directional flexibility.

The website analysis highlighted where cybersecurity information is published by organisations and found that, because there is no legal obligation to disclose, very little is made public, despite the emergence of a potential social obligation. Analysis of the websites was made easier using Microsoft Excel and NVivo12. However, I found NVivo 12 difficult to use at first, and only found acceptable proficiency following formal training. NVivo 12 was also used in the analysis of the interviews, and proved

to be a powerful tool when searching for qualitative understanding. Extracting qualitative observations and grouping them for thematic analysis brought deeper understanding of the participants' opinions, and when combined with the results of the website analysis, they helped to answer the research questions. While the answers to those research questions are important, it is the practical application of that knowledge that has the greatest value. For example, the first research question enquires how DDoS is rated and evaluated. Through interviews, the study found that while DDoS is rated as a high threat, it does not rank as high as data loss or reputational damage. In addition, this rating was achieved through estimations by individuals and internal groups rather than through external subject matter experts or via formal risk frameworks. However, when combined with the website analysis results, deeper understanding began.

With low amounts of cybersecurity information published by organisations and almost no public self-reporting of incurred cybersecurity attacks, organisations may be demonstrating their fear of the reputational damage that is associated with victim status (Buil-Gil et al., 2021). Reputational damage was a fear that was stated by many participants, so it is likely that they seek to prevent leakage of damage or attacks to prevent public awareness. Unfortunately, while this strategy may succeed in one area (reputational protection), it may be detrimental in the area of capability improvements. The hesitancy to share information (including internally) can be damaging, as knowledge sharing and collaboration often lead to overall better capability. Groups perform better than single minds; therefore, by limiting the release of experience to save reputation, they may effectively limit their ultimate capability. Another research question looked at how Australian organisations could be more prepared for a DDoS event, and how different groups could influence this transition. Here, the theme of collaboration continued.

Looking from the bottom up, it is the individual participants who are requesting more access to training and collaboration. As mentioned above, for cybersecurity, organisations rely on their own skills and experience rather than external expertise and formal frameworks, and this constricts their capability. When their cybersecurity departments obscure their operations from the rest of the organisation, this capability is restricted even further, and this contradicts what we know regarding the benefits of

greater diversity for teamwork, development and innovation. With greater access to information and experiences of others, employees would be in possession of the evidence they need to drive organisational change. How else can we expect employees and organisations to be aligned when collaboration is restricted in this way?

From the top down, governments hold substantial amounts of cybersecurity intelligence (ASD) and the power to drive national change. The ACCC already enforces regulations that prevent the sale of flammable nightwear (Australian Consumer Law, 2016), thus preventing us from "going up in flames". As participants overwhelmingly stated loss of data (e.g., PII, PHI and intellectual property) was their greatest concern, why not extend this perspective to our digital shadow? It is within the government's power to create new legislation for minimum standards of cybersecurity in products and provide the governance to ensure standards are maintained. They just need incentive to do this.

In the middle sits the industry vendors and service providers who produce the technology products that individuals, organisations and governments use and supply the training for those products and approaches to implementation. Innovation in these industries is driven by investor expectations, but they must also conform to consumer demand and government legislation. Therefore, ultimately, it can be that individuals hold the power to make change. Through collaboration, it is the individual who is able to influence organisations to adjust their thinking and through voting power, they can influence governments to build further legislation and governance. Therefore, pressure from above and below gives individuals the potential power to drive industry to develop greater cybersecurity in their products and drive greater cybersecurity awareness overall.

7.2 Limitations

Reflecting on the study journey, several limitations were prominent. First of these is the scale of the study. While it would not be possible to interview all the employees in Australian organisations, the number of participants represents only a small slice of the Australian workforce. In part, this may be due to inaccurate assumptions, as my assumption was that, if anonymised, employees would feel at ease talking about cybersecurity; however, this was not reflected in the participant response statistics

(Figure 5.8), where only 27% agreed to proceed and were interviewed. This limitation may be a reflection of Australian culture and may not be the same if the research were conducted in another country.

Choosing interviews as a method of data collection may also have had an effect. Compared to other methods (e.g., short surveys), semi-structured interviews demand more time from the participant and can be much more emotionally engaging than indirect surveys. In addition, DDoS as a cybersecurity subject matter tends to be confidential, and as demonstrated by the results of this study, cybersecurity is something organisations do not feel comfortable to share. Therefore, with the two issues combined, it was quickly evident that this assumption was inaccurate. However, the nature of exploratory research allowed me to adapt my data collection methods and choose the best option for the circumstances. Hindsight, however, does present the opportunity to reflect, and other options in the future may be more appropriate if the study were to be repeated.

A second limitation of diversity became apparent through the results. The majority of interviewees were male. It is unclear why this was, but the statistics in this study did not align with the most recent gender diversity results from the ABS (2022). Also, fewer females were approached but more females accepted the invitation, which potentially may be evidence of a limitation in my approach to finding willing participants and is something that future studies should consider if they follow similar methods to this approach.

A third limitation was the impact of the COVID-19 pandemic that reached Australia late in 2019. It was not a limitation of the methods used in the study, but it was a limiting factor during data collection. As employees were adopting a new normality, not knowing if this new regime was to be a temporary or permanent reality, they struggled with the change of working arrangements, isolation and uncertainty. For this study, this created difficulties in arranging face-to-face interviews and alternate arrangements had to be considered. Of the remaining options considered (videoconference, phone, or survey), it was videoconference that could most positively transmit the social clues that are a vital part of my interviewing technique. However, despite adjusting to this non-natural communication method, I found

interviewing this way to be more awkward than face-to-face interviewing; therefore, the quality of these interviews may have been lower than if performed in person.

7.3 Significance

The overarching aim for this research study was to demystify perceptions of the DDoS risk and threat within Australian organisations. However, the significance of this study can be seen in two areas. One is as a contribution to academic research through the development of new knowledge, while the other is to positively influence social change within Australian organisations so that they may lead the practical thinking of how governments and industry build their strategies to cope with DDoS and other cybersecurity events.

Academically, this thesis should stand as a stepping stone for future researchers to use to build their knowledge in this and associated or compatible research projects. It is intended that the results and methods used within be made available and be adapted, discussed and considered as part of any future projects.

Socially, through dissemination, these results could begin to influence employees in organisations and help them to understand that the value of sharing knowledge and experiences can be more than the impact of victim-created reputational loss. This small step may be the first in a long path towards a more effective cybersecurity strategy, greater product security and a change in the balance of power between cyber-attackers and defenders.

7.4 Recommendations and Future Work

The recommendations of this study are led by the implications that were discussed in Section 6.6. On a practical and social level, this study showed that little cybersecurity information is shared within and between organisations, and even less is publicly released. This lack of collaboration may have a detrimental effect on organisational capabilities, and this was a common theme throughout the interviews. As discussed in Section 6.6.1, diverse cultural collaboration can bring greater capability, but there is a risk that individuals may follow their own needs and views when undertaking cybersecurity tasks. It is therefore important that employees are integrated into an

organisation's culture so that their actions align with pre-defined cybersecurity strategies. However, with a lack of communication and collaboration as mentioned in the interviews, this alignment may fail to achieve optimal levels.

In a similar way, inter-organisational collaboration is also lacking. Unable to pool ideas, learn from the experience others and see problems from alternate perspectives, the organisational community as a whole could unknowingly restrict its own capability. It is therefore recommended that organisations begin to critically examine their own levels of collaborative performance and actively pursue new ways to adeptly share useful experiences and knowledge while retaining security of sensitive information.

Along with a push to raise collaborative efforts, organisations should also begin to encourage industry and government to bring in standards for network-connectable products. However, as discussed in Section 6.6.1, standards in products should be accompanied by simplistic configuration methods. Therefore, through their newly established collaborative methods, organisations should take the lead in developing new ways to configure network devices, such as by automation, AI and ML.

From a policy point of view, any product standards introduced into legislation must be accompanied by governing processes to ensure they are adhered to. Organisations should engage government to begin developing this policy, but the government can do more. Similar to the Repository of Industrial Security Incidents (RISI, 2015), a national database of cyber-attacks on Australian organisations would bring an in-depth and longitudinal body of knowledge to the fingertips of academic and practitioner cybersecurity researchers.

From a theoretical perspective, more research should be performed on the motivations and drivers of individuals within a cyber-security context. While there are beginnings of research in this area and studies into human motivations, a new area of interest could be to develop ways to positively exploit behavioural patterns to benefit cyber-security implementation. However, any future research should learn from the experiences of others who conducted research through COVID-19. Methodologically, COVID-19 highlighted the difficulties future researchers may face, such as the increased likelihood of working with remote teams, the technology challenges that

may create and that face-to-face communication may be the exception, rather than normality. Future researchers in this area should consider this in their plans and find new ways to engage participants more effectively.

References

A10 Networks. (2022, March 11). *What is a volumetric DDoS attack?* https://www.a10networks.com/glossary/what-is-a-volumetric-ddos-attack/

Abdollahi, A., & Fathi, M. (2020). An intrusion detection system on ping of death attacks in IoT networks. *Wireless Personal Communications, 112*, 2057-2070. https://doi.org/10.1007/s11277-020-07139-y

Abrams, S. E. (2012, Apr 19). Purpose, insight, and the review of literature. *Public Health Nursing, 29*(3), 189-190.

Abreu, P. (2017, Nov 15). *Why manufacturers make insecure IoT devices and how you can protect them*. IOT Agenda https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Why-manufacturers-make-insecure-IoT-devices-and-how-you-can-protect-them

Abukari, A. M., & Bankas, E. (2020, May). Some cyber security hygienic protocols for teleworkers in covid-19 pandemic period and beyond. *International Journal of Scientific and Engineering Research, 11*(4), 1401-1407. https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond

ACSM_Admin. (2019, June 5). *Corporate cyber breaches increasing in Australia, with people-based attacks up by a third*. Australian Cyber Security Magazine https://australiancybersecuritymagazine.com.au/corporate-cyber-breaches-increasing-in-australia-with-people-based-attacks-up-by-a-third/

Academic Ranking of World Universities. (2018). *2018 statistics.* http://www.shanghairanking.com/ARWU-Statistics-2018.html

Adams, T., & Scolland, S. (2006). *Internet effectively. A beginner's guide to the world wide web.* Pearson Education Inc.

Adams, W. C. (2015). *Conducting semi-structured interviews.* Wiley.

Agee, J. (2009). Developing qualitative research questions: A reflective process. *International Journal of Qualitative Studies in Education, 22*(4), 431-447.

Agence France-Presse. (2016, Nov 15). *Man 'who almost broke the internet' escapes jail*. ABS-CBN News https://news.abs-cbn.com/overseas/11/14/16/man-who-almost-broke-the-internet-escapes-jail

Aghion, P., & Jackson, M. O. (2016). Inducing leaders to take risky decisions: Dismissal, tenure, and term limits. *American Economic Journal: Microeconomics, 8*(3), 1-38. https://doi.org/10.1257/mic.20150083

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1). https://doi.org/10.1093/cybsec/tyy006

Ahmad, R. Y. (2012). Perception on cyber terrorism: A focus group discussion approach. *Journal of Information Security, 3*(3), 231-237.

Ahmed, I., & Roussev, V. (2018). Peer instruction teaching methodology for cybersecurity education. *IEEE Security and Privacy Magazine, 16*(4), 88-91. https://doi.org/10.1109/MSP.2018.3111242

Akamai. (2016). *Akamai's [state of the internet] / security.* https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf

Akamai. (2020). *Akamai's [state of the internet] / security.* https://www.akamai.com/content/dam/site/en/documents/state-of-the-internet/soti-security-a-year-in-review-report-2020.pdf

Akhter, F., Khadivizand, S., Siddiquei, H. R., Alahi, M. E., & Mukhopadhyay, S. (2019). IoT enabled intelligent sensor node for smart city. *Sensors, 19*(15), 3374-. https://doi.org/10.3390/s19153374

Aladenusi, T. (2020, March 25). *COVID-19's impact on cybersecurity*. Deloitte. https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html

Alagaraja, M., & Shuck, B. (2015). Exploring organizational alignment-employee engagement linkages and impact on individual performance: A conceptual model. *Human Resource Development Review, 14*(1), 17-37. https://doi.org/10.1177/1534484314549455

Aleroud, A., & Zhou, L. (2017, July). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160-196. https://doi.org/10.1016/j.cose.2017.04.006.

Allison, J., Horner, R., &Kiefe,C. (2018). *Personal Bias in Scientific Review*. Medical Care, 56 (4), 279-280. doi: 10.1097/MLR.0000000000000892.

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing, 25*(5), 829-841. https://doi.org/10.1007/s00779-021-01551-2

Amazon Web Services. (2019, May 3). *Amazon Route 53.* https://aws.amazon.com/route53/

Amazon Web Services. (2022, January 3). *Shared responsibility model.* https://aws.amazon.com/compliance/shared-responsibility-model/

Anandarajan, M., & Lippert, S. K. (2006). Competing mistresses? Academic vs. practitioner perceptions of systems analysis. *Journal of Computer Information Systems, 46*(5), 114-126.

Anderson, I. (2021, June 20). *Cyber resilience: Inquiry into auditor-general's Report 1 and 13 (2019-20).* Parliament of Australia. https://www.aph.gov.au/DocumentStore.ashx?id=51e4a26c-15e8-4ce4-9296-5f43dcf39e83

Anstee, D., Chui, C. F., Bowen, P., & Sockrider, G. (2017, January 24). *Worldwide infrastructure security report.* Arbor Networks https://www.astrid-online.it/static/upload/12th/12th_worldwide_infrastructure_security_report.pdf

Antoniou, S. (2009, May 14). *The ping of death and other DoS network attacks.* Pluralsight. https://www.pluralsight.com/blog/it-ops/ping-of-death-and-dos-attacks

Arquilla, J., & Ronfeldt, D. (1997). *In Athena's camp preparing for conflict in the information age.* Rand. https://www.rand.org/pubs/monograph_reports/MR880.html

Arthur, C. (2013, March 29). *Undersea internet cables off Egypt disrupted as navy arrests three.* The Guardian. https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests#:~:text=Egyptian%20naval%20forces%20have%20arrested,capacity%20between%20Europe%20and%20Egypt.

Arzoomanian, R. (2009, June 26). *A complete history of mainframe computing*. Toms Hardware. https://www.tomshardware.com/picturestory/508-mainframe-computer-history.html

ASD. (2020, July 27). *Cloud computing aecurity considerations*. Australian Cyber Security Centre: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations

ASD. (n.d.). *Australian Cyber Security Centre*. https://www.cyber.gov.au/

Asghar, J. (2013). Critical paradigm: A preamble for novice researchers. *Life Science, 10*, 3121-3127.

Ashford, W. (2016, February 1). *DDoS is most common cyber attack on financial institutions.* Computer Weekly.com https://www.computerweekly.com/news/4500272230/DDoS-is-most-common-cyber-attack-on-financial-institutions

Associated Press. (2019a, December 14). *Large hospital system hit by ransomware attack.* Security Week. https://www.securityweek.com/large-hospital-system-hit-ransomware-attack

Associated Press. (2019b, October 03). *Alabama hospital system halts admissions amid malware attack.* Security Week: https://www.securityweek.com/alabama-hospital-system-halts-admissions-amid-malware-attack

Associated Press. (2019c, September 23). *Wyoming Hospital's services disrupted by ransomware.* Security Week. https://www.securityweek.com/wyoming-hospitals-services-disrupted-ransomware

Associated Press. (2020, September 17). *German hospital hacked, patient taken to another city dies.* Security Week. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies

Atwood, J. (2006, September 20). *Fifty years of software development*. Coding Horror. https://blog.codinghorror.com/fifty-years-of-software-development/

AustCyber. (2019). *Sector competiveness plan.* https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3

Australian Bureau of Statistics. (2010, May 28). *8155.0 - Australian industry, 2008-09.* https://www.abs.gov.au/ausstats/abs@.nsf/Products/8155.0~2008-09~Glossary~Glossary?OpenDocument

Australian Bureau of Statistics. (2015, October 29). *5204.0 - Australian system of national accounts, 2013-14.*

http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/5204.02013-14?OpenDocument

Australian Bureau of Statistics. (2018, September 29). *4125.0 - Gender indicators, Australia, Sep 2018*. https://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/4125.0~Sep%202018~Main%20Features~Economic%20Security~4

Australian Bureau of Statistics. (2020a, February 20). *8165.0 - Counts of Australian businesses, including entries and exits, June 2015 to June 2019*. https://www.abs.gov.au/ausstats/abs@.nsf/mf/8165.0

Australian Bureau of Statistics. (2020b, December 15). *Gender Indicators, Australia* . Retrieved from Australian Bureau of Statistics: https://www.abs.gov.au/statistics/people/people-and-communities/gender-indicators-australia/latest-release

Australian Bureau of Statistics. (2021, July 16). *What the census is*. https://www.abs.gov.au/census/learn/about

Australian Bureau of Statistics. (2022). *EQ09 - Employed persons by industry division (ANZSIC) and occupation major group (ANZSCO) of main job and sex, August 1986 onwards (pivot table)*. https://www.abs.gov.au/statistics/labour/employment-and-unemployment/labour-force-australia-detailed/feb-2022/EQ09.xlsx

Australian Computer Science Week. (2022). *Conference Proceedings*. https://acsw.org.au/

Australian Competition and Consumer Commission. (2021, July 6). *Your rights & responsibilities as a business online*. https://www.accc.gov.au/business/business-rights-protections/your-rights-responsibilities-as-a-business-online

Australian Consumer Law. (2016). *Consumers and the ACL*. https://consumer.gov.au/consumers-and-acl

Australian Cyber Security Centre. (2021). *Essential eight maturity model*. https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

Australian National University. (2019, October 2). *ANU releases detailed account of data breach*. https://www.anu.edu.au/news/all-news/anu-releases-detailed-account-of-data-breach

Australian Small Business and Family Enterprise Ombudsman. (2017, March 28). *Small business statistical report - Final.* https://www.asbfeo.gov.au/sites/default/files/Small_Business_Statistical_Report-Final.pdf

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* International Conference on Cyber Security for Sustainable Society. https://arxiv.org/abs/1901.02672

Baker, J. D. (2016). The purpose, process, and methods of writing a literature review. *AORN Journal, 103*(3), 265-269.

Bartunek, J. M., & Rynes, S. L. (2014, May 23). *The gap between academics and practitioners is a reflection of the underlying tensions of academic belonging.* LSE. https://blogs.lse.ac.uk/impactofsocialsciences/2014/05/23/the-paradoxes-of-academic-and-practitioner-relationships/

Baruch, Y. (1999). Response rate in academic studies - A comparative analysis. *Human Relations*. 52(4), 421-438. https://doi.org/10.1023/A:1016905407491

Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2021). *Data breach investigations report: Summary of findings*. Verizon. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/summary-of-findings/

Baxter, M. (2021, July 17). *Forget Moore's Law - we need Koomey's Law says ARM director*. Techopian. https://www.techopian.com/forget-moores-law-we-need-and-koomeys-law-says-arm-director/

Bdair Alghuraibawi, A., Rosni , A., Manickam, S., Alkareem, A., & Zaid, A. (2021). Detection of ICMPv6-based DDoS attacks using anomaly based intrusion detection system: A comprehensive review. *International Journal of Electrical and Computer Engineering, 11*(6), 5216-5228. https://doi.org/10.11591/ijece.v11i6.pp5216-5228

Beato, F., Gumbiner, A., Simonovich, L., & Al-Zamil, W. (2021). *Cyber resilience in the oil and gas industry: Playbook for boards and corporate officers.* World Economic Forum. https://www3.weforum.org/docs/WEF_Board_Principles_Playbook_Oil_and_Gas_2021.pdf

Bendemra, H. (2013, Oct 29). *Doing a PhD can be a lonely business but it doesn't have to be*. The Conversation. http://theconversation.com/doing-a-phd-can-be-a-lonely-business-but-it-doesnt-have-to-be-19192

Bender, H. (2014, Sept 12). *5 most targeted industries for DDoS attacks*. Property Casualty 360. http://www.propertycasualty360.com/2014/09/12/5-most-targeted-industries-for-ddos-attacks?t=information-security&page=2&slreturn=1515929809

Bermudez Villalva, D. A., Onaolapo, J., Stringhini, G., & Musolesi, M. (2018). Under and over the surface: A comparison of the use of leaked account credentials in the dark and surface web. *Crime Science, 7*(1), 1-11. https://doi.org/10.1186/s40163-018-0092-6

Berni, L. (2016, December 14). *Cybercriminals and activists scale up their attacks – who's at risk and why?* Control Risks. https://www.controlrisks.com/our-thinking/insights/cybercriminals-and-activists-scale-up-their-attacks

Bettis, R. A., Gambardella, A., Helfat, C., & Mitchell, W. (2014). Qualitative empirical research in strategic management. *Strategic Management, 36*(1), 637-639.

Bienkowski, Y. (2016, Aug 2). *Denial of service & denial of access: Living in an era of cyber extortion*. Arbor Networks. https://www.arbornetworks.com/blog/insight/denial-service-denial-access-living-era-cyber-extortion/

Birkman International. (2016). *How generational differences impact organizations & teams.* https://birkman.com/wp-content/uploads/2016/05/Generational-Differences-PDF.pdf

Blythe, J. J. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science, 9*(1), 1. https://doi.org/10.1186/s40163-019-0110-3

Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science, 9*, 1. https://doi.org/10.1186/s40163-019-0110-3

Bock, K., Alaraj, A., Fax, Y., Hurley, K., Wustrow, E., & Levin, D. (2021, August 11-13). Weaponizing middleboxes for TCP reflected amplification. In *Proceedings of 30th USENIX Security Symposium* (pp. 3345-3361). USENIX Association. https://geneva.cs.umd.edu/papers/usenix-weaponizing-ddos.pdf

Bondarenko, P. (2018, May 27). *Secure second strike*. Britannica. https://www.britannica.com/topic/second-strike-capability

Börger, T. (2012). *Social desirability and environmental valuation.* Frankfurt.

Bosse, D. A., & Phillips, R. A. (2016). Agency theory and bounded self-interest. *Academy of Management Review, 41*(2), 276-297. https://doi.org/10.5465/amr.2013.0420

Bourgue, R., Budd, J., Homola, J., Wlasenko, M., & Kulawik, D. (2013, November 20). *Detect, share, protect: Solutions for improving threat data exchange among CERTs.* ENISA. https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

Bowen, M. (2021, December 1). *Southern Cross NEXT submarine cable to complete journey in Coogee*. Intelligent CIO. https://www.intelligentcio.com/apac/2021/12/01/southern-cross-next-submarine-cable-to-complete-journey-in-coogee/#

Bowman, E. (2021, April 9). *After data breach exposes 530 million, Facebook says it will not notify users*. NPR. https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users

Brenner, S. B. (2009). *Cyberthreats: The emerging fault lines of the nation state.* Oxford University Press.

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace.* ABC-CLIO, LLC.

Brilingaitė, A., Bukauskas, L., & Juozapa, A. (2022). Overcoming information-sharing challenges in cyber defence exercises. *Journal of Cybersecurity, 8*(1). https://doi.org/10.1093/cybsec/tyac001

Brisson, M.-N., & Savoie, M. (2018). Cybersecurity oversight and strategy for commercial real estate: Fundamentals of cybersecurity oversight and risk management. *Real Estate Issues, 42*(2), 1-4.

Britz, M. T. (2013). *Computer forensics and cyber crime: An introduction* (3rd ed.). Pearson.

Buffered. (2018, February). *What is ping of death*. https://buffered.com/glossary/ping-of-death/

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention.

Victims & Offenders, 16(3), 286-315. https://doi.org/10.1080/15564886.2020.1814468

Butun, I., Pereira, N., & Gidlund, M. (2018). Security risk analysis of LoRaWAN and future directions. *Future Internet, 11*(1), 3. https://doi.org/10.3390/fi11010003

Campbell, N. (2018, August 13). *Industry focus on security grows as threat of cybercrime increases*. Australian Cyber Security Magazine. https://australiancybersecuritymagazine.com.au/industry-focus-on-security-grows-as-threat-of-cybercrime-increases/

Cappellino, M. (2014, June 26). *Every conversation could use a preamble*. https://markcappellino.com/blog/conversation-preamble/

Carneiro, L., & Johnston, M. (2014). Quantitative and qualitative visual content analysis in the study of websites. SAGE. https://doi.org/10.4135/9781446273050135178 00.

Cassard, A., & Hamel, J. (2018). Exponential growth of technology and the impact on economic jobs and teachings: Change by assimilation. *Journal of Applied Business and Economics, 20*(2), 76-81.

CDNetworks. (2017). *Q2 2017 DDoS attack trends report*. https://www.cdnetworks.com/sg/resources/CDNetworks_DDoS%20Attack%20Trends_Q2%202017_ENG_final_20170821-2-.pdf

Chadd, A. (2018). DDoS attacks: Past, present and future. *Network Security*, *2018*(7), 13-15.

Chamorro-Premuzic, T. (2013, October 25). ThefFive characteristics of successful innovators. *Harvard Business Review*. https://hbr.org/2013/10/the-five-characteristics-of-successful-innovators

Chan, H. W., Russell, A. M., & Smith, M. Y. (2018). What is the quality of drug safety information for patients: An analysis of REMS educational materials. *Pharmacoepidemiology & Drug Safety*, *27*(9), 969-978. https://doi.org/10.1002/pds.4614

Chandler, D. L. (2013, March 6). *How to predict the progress of technology*. MIT News. http://news.mit.edu/2013/how-to-predict-the-progress-of-technology-0306

Chapelle, A. (2019). *Operational risk management: Best practices in the financial services industry*. John Wiley & Sons.

Chapman, P. (2020). Are your IT staff ready for the pandemic-driven insider threat? *Science Direct*, *2020*(4), 8-11. https://doi.org/10.1016/S1353-4858(20)30042-8

Chaudhry, T., (2022). State backed cyber-attack exclusions. Lloyds. https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf

Chauhan, A. S. (2018). *Practical network scanning : Capture network vulnerabilities using standard tools such as Nmap and Nessus.* Packt Publishing Limited.

China Correspondent. (2013, March 15). *The Great Firewall of China*. OpenDemocracy. https://www.opendemocracy.net/en/great-firewall-of-china/

Chipeta, C. (2021, November 14). *ISO 27001 implementation checklist*. Up Guard. https://www.upguard.com/blog/iso-27001-implementation-checklist

Chittester, C. G., & Haimes, Y. Y. (2004). Risks of terrorism to information technologyand to critical interdependent infrastructures. *Journal of Homeland Security and Emergency Management, 1*(4), 1-20. https://doi.org/10.2202/1547-7355.1075

Cicmil, S., Williams, T., Thomas, J., & Hodgson, D. (2006). Rethinking project management: Researching the actuality of projects. *International Journal of Project Management, 24*(8), 675-686. https://doi.org/10.1016/j.ijproman.2006.08.006

Cimpanu, C. (2019a, January 10). *Anonymous hacker gets 10 years in prison for DDoS attacks on children's hospitals*. ZDNet. https://www.zdnet.com/article/anonymous-hacker-gets-10-years-in-prison-for-ddos-attacks-on-childrens-hospitals/

Cimpanu, C. (2019b, December 4). *China resurrects Great Cannon for DDoS attacks on Hong Kong forum*. ZDNet. https://www.zdnet.com/article/china-resurrects-great-cannon-for-ddos-attacks-on-hong-kong-forum/

Cimpanu, C. (2020, January 28). *LoRaWAN networks are spreading but security researchers say beware*. ZDNet. https://www.zdnet.com/article/lorawan-networks-are-spreading-but-security-researchers-say-beware/

Cybersecurity and Infrastructure Security Agency. (2009, November 4). *Security tip (ST04-015) - Understanding Denial-of-Service attacks*. CISA. https://www.us-cert.gov/ncas/tips/ST04-015

Cisco. (2020, May 21). *AI and machine learning: A technology overview for business decision makers*. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-cisco-dna-ai-ml-primer-cte-en.html

Clarke, R. A., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* Harper Collins.

Clarke, V., & Braun, V. (2017). Thematic analysis. *Journal of Positive Psychology, 12*(3), 297-298. https://doi.org/10.1080/17439760.2016.1262613

Cloudflare. (2019, October 2). *Famous DDoS attacks: The largest DDoS attacks of all time*. https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

Coenders, G. (2017, May 9). *Weaponizing the IoT for DDoS attacks*. Interconnections - The Equinix Blog. https://blog.equinix.com/blog/2017/05/09/weaponizing-the-iot-for-ddos-attacks/

Cohen, M. S. (2018). *Beyond theory: Applying empirical evidence to cyberspace theories* [Unpublished PhD thesis]. Northeastern University.

Cole, B. (2019, April). *How information sharing can reduce cybersecurity vulnerabilities*. Tech Target. https://www.techtarget.com/searchsecurity/feature/How-information-sharing-can-reduce-cybersecurity-vulnerabilities

Competition and Consumer Act 2010.

CompTIA. (2021, December). *CompTIA certifications*. https://www.comptia.org/certifications

Conrad, J. (2011). Interstate rivalry and terrorism: An unprobed link. *Journal of Conflict Resolution, 55*(4), 529-555.

Constantin, L. (2015, May 12). *Update: malware-infected home routers used to launch DDoS attacks*. Computer World. https://www.computerworld.com/article/2921559/malware-infected-home-routers-used-to-launch-ddos-attacks.html

Constantin, L.. (2021, May 18). *DDoS attacks: Stronger than ever and increasingly used for extortion*. CSO Australia. https://www.csoonline.com/article/3618411/ddos-attacks-stronger-than-ever-and-increasingly-used-for-extortion.html

Consultores, B. (2021, May 18). *Axiology in research*. Online Tesis. https://online-tesis.com/en/axiology-in-research/

Control Risks. (2017, November 2). *The rise of cyber extortion*. https://www.controlrisks.com/our-thinking/insights/the-rise-of-cyber-extortion

Cooksey, R., & McDonald, G. (2011). *Surviving and thriving in postgraduate research.* Tilde University Press.

Coombs, W. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*. https://doi.org/10.1057/palgrave.crr.1550049

Corero. (2016). Loss of customer trust and decreased revenues most damaging consequences of DDoS attacks. *Database and Network Journal, 46*(2), 9.

Costello, P. (2003). *Action research.* Bloomsbury Publishing Plc.

Council on Foreign Relations. (2005, August). *Titan rain*. https://cfr.org/

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (US). https://www.congress.gov/bill/98th-congress/house-bill/5112

Cox, L. A. (2008). What's wrong with risk matrices? *Risk Analysis, 28*(2), 497-512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Credeur, M. J. (2002, Jul 22). EarthLink wins $25 million lawsuit against junk e-mailer. *Atlanta Business Chronical*. https://www.bizjournals.com/atlanta/stories/2002/07/22/story4.html

Center for Strategic and International Studies. (2022). *Significant cyber incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

CubCyber. (2020, September 16). *14 year old boy takes down Amazon, CNN, Yahoo!, and eBay. Also CMMC and DDoS attacks*. https://www.cubcyber.com/14-year-old-takes-down-amazon-cmmc-and-ddos

Cucu, P. (2019, April 23). *How to DDoS like an ethical hacker*. Heimdal. https://heimdalsecurity.com/blog/how-to-ddos/

Cunningham, C. (2020). *Cyber warfare - Truth, tactics, and strategies.* Packt Publishing.

CX Central. (2020, February 27). *Australian businesses falling behind in AI adoption*. https://cxcentral.com.au/industry-news/ai-adoption/

Cyber Security CRC. (2021). *Who we are*. https://cybersecuritycrc.org.au/who-we-are

Cyber Security Masters Degree. (2018, May 21). *How the 80s classic War Games inspired a generation of hackers and cybersecurity pros*. https://www.cybersecuritymastersdegree.org/2018/05/how-the-80s-classic-war-games-inspired-a-generation-of-hackers-and-cybersecurity-pros/

CyberEdge Group. (2017). *2017 cyberthreat defense report*. https://cyber-edge.com/resources/cyberedge-2017-cyberthreat-defense-report/

CyberEdge Group. (2020). *2020 cyberthreat defense report*. https://cyber-edge.com/resources/2020-cyberthreat-defense-report/

CYBSafe. (2018, December 19). *Remote working poses significant security risk to UK's SME businesses, new research reveals*. https://www.cybsafe.com/press-releases/remote-working-poses-significant-security-risk-to-uks-sme-businesses-new-research-reveals/

Da Veiga, A., Martins, N., & Eloff, J. (2007). Information security culture – validation of an assessment instrument. *Southern African Business Review, 11*(1), 147-166.

Dan, A. (2019, April 16). *Ecuador claims it suffered 40 million cyber attacks since Julian Assange's arrest*. Tech The Lead. https://techthelead.com/ecuador-claims-it-suffered-40-million-cyber-attacks-since-julian-assanges-arrest/

Daniel, H. (2014, March 20). *Doctor of philosophy rules*. UNE. https://policies.une.edu.au/download.php?id=112&version=1

Daws, R. (2019, January 14). *British hacker took down Liberia's whole telecoms network*. Telecoms Tech News. https://www.telecomstechnews.com/news/2019/jan/14/british-hacker-liberia-telecoms-network/

De Bruin, L. (2016, September 18). *Scanning the environment: PESTEL analysis*. Business To You. https://www.business-to-you.com/scanning-the-environment-pestel-analysis/

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2019). *Enterprise governance of information technology: Achieving alignment and value in digital organizations.* Springer.

Del Marmol, T., Feys, B., & Probert, C. (2015). *Pestle analysis*. Lemaitre Publishing.

Delibasic, S. (2018, August 30). *Australian universities bombarded by foreign hackers*. The New Daily. https://thenewdaily.com.au/life/tech/2018/08/30/universities-cyber-attacks/

Dennis, D. (2010, February 11). Perhaps the first Denial-of-Service attack? Plato History. http://www.platohistory.org/blog/2010/02/perhaps-the-first-denial-of-service-attack.html

Department of Justice. (2021, August 11). *Fintech CEO sentenced to 6 years in prison for multiple fraud schemes, including $7 million covid-19 pandemic loan fraud and securities fraud*. https://www.justice.gov/usao-sdny/pr/fintech-ceo-sentenced-6-years-prison-multiple-fraud-schemes-including-7-million-covid

Department of the House of Representatives. (2018). *House of Representatives practice* (7th ed.). Parliament of Australia. https://www.aph.gov.au/-/media/05_About_Parliament/53_HoR/532_PPP/Practice7/Prelims/7Prelims.pdf?la=en&hash=BA4E486C1445FAB45A2037C21318333A2E3FDC37

Deschamps, R. (2018, September 7). *Can I collect research data before writing a literature review chapter?* Quora. https://www.quora.com/Can-I-collect-research-data-before-writing-a-literature-review-chapter

Diaconu, M. (2016). Insights on education – Innovation links and impact. *Revista Română de Statistică, 64*(1), 81-96. https://www.revistadestatistica.ro/wp-content/uploads/2016/03/RRS01_2016_A7.pdf

Dilmegani, C. (2021, August 2). *84 chatbot /conversational AI statistics: Market size, adoption*. AI Multiple. https://research.aimultiple.com/chatbot-stats/

Djuraskovic, I., & Arthur, N. (2010). Heuristic inquiry: A personal journey of acculturation and identity reconstruction. *The Qualitative Report, 15*(6), 1569-1593.

Dobson, S. (2004). *The triple constraints in project management.* Management Concepts. Inc.

Dudek, S. (2021, January 26). *Low powered and high risk: Possible attacks on LoRaWAN devices*. Trend Micro. https://www.trendmicro.com/en_au/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html

Duncan, R. (2020). What does ‘secure by design’ actually mean? *Network Security, 2020*(8), 18-19. https://doi.org/10.1016/S1353-4858(20)30095-7

Durey, A. (2022). *Selling out: How powerful industries corrupt our democracy*. https://static1.squarespace.com/static/580025f66b8f5b2dabbe4291/t/61f75c0ba71fd75a58d9f036/1643600956345/Selling+Out+How_powerful+industries+corrupt+our+democracy_31_Jan.pdf

Dworkin, S. L. (2012). Sample Size Policy for Qualitative Studies Using In-Depth Interviews. *Archives of Sexual Behavior*, 41(6), 1319–1320. https://doi.org/10.1007/s10508-012-0016-6

EC-Council. (2021, January). *Cyber security programs*. https://www.eccouncil.org/programs/

Eeckhout, L. (2017). Is Moore's Law slowing down? What's next? *IEEE Micro, 37*, 4-5. https://doi.org/10.1109/MM.2017.3211123

Ellimoottil, C., Polcari, A., & Gupta, G. (2012, Dec). Readability of websites containing information about prostate cancer treatment options. *Journal of Urology, 188*(6), 2171-2176. https://www.sciencedirect.com/science/article/abs/pii/S0022534712044114

ENISA. (2016). *Report on cyber security information sharing in the energy sector*. https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector

Ertan, C. G., Heath, C., Denny, D., & Jensen, R. (2020). *Cyber security behaviour in organisations.* Arxiv. https://arxiv.org/ftp/arxiv/papers/2004/2004.11768.pdf

Eubank, W., & Weinberg, L. (2001). Terrorism and democracy: Perpetrators and victims. *Terrorism and Political Violence, 13*, 155-164.

Evans, D. (2011, April). *The Internet of Things: How the next evolution of the internet is changing everything.* Cisco. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Farwell, J. P. (2011). Stuxnet and the future of cyber war. *Survival, 53*(1), 23-40.

Fazzini, K., & DiChristopher, T. (2019, May 2). *An alarmingly simple cyberattack hit electrical systems serving LA and Salt Lake, but power never went down*. CNBC. https://www.cnbc.com/2019/05/02/ddos-attack-caused-interruptions-in-power-system-operations-doe.html

Fenil, E., & Kumar, P. M. (2019). Survey on DDoS defense mechanisms. *Concurrency and Computation Practice and Experience*, *32*(6), e5114. https://doi.org/10.1002/cpe.5114

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2007). *Role-based access control* (2nd ed.). Artech House.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86*, 13-23. https://doi.org/10.1016/j.dss.2016.02.012

Findley, M. G. (2012). Games rivals play: Terrorism in international rivalries. *Journal of Politics, 74*(1), 235-248.

Fipps, P. (2018, March 29). *Notice of data breach*. MyFitnessPal. https://content.myfitnesspal.com/security-information/notice.html

Flesch, R. (1996). *How to write plain English*. University of Canterbury. http://www.mang.canterbury.ac.nz/writing_guide/writing/flesch.shtml

Flick, U. (2007). *Managing quality in qualitative research*. SAGE Publications, Ltd. https://doi.org/10.4135/9781849209441.n4

Foltýn, T. (2019, Jun 4). *Hackers steal 19 years' worth of data from a top Australian university*. We Live Security. https://www.welivesecurity.com/2019/06/04/data-stolen-australia-university/

Foltz, C. B. (2004). Cyber terrorim, computer crime, and reality. *Information Management & Computer Security, 12*(2), 54-166. https://doi.org/10.1108/09685220410530799

Fontana, A., & Frey, J. H. (1994). The art of science. In N. Denzin & Y. Lincoln (Eds.), *The handbook of qualitative research* (pp. 361-376). Sage Publications. http://jan.ucc.nau.edu/~pms/cj355/readings/fontana%26frey.pdf

Forrest, C. (2018, August 15). *Why Israel is investing $24M in its cybersecurity industry*. Tech Republic. https://www.techrepublic.com/article/why-israel-is-investing-24m-in-its-cybersecurity-industry/

Fortinet. (2017, January 4). *DDoS-attack-mitigation-demystified*. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/DDoS-Attack-Mitigation-Demystified.pdf

Foster, J. (2018). Planning for instead of reacting to disasters. *Agency Sales, 48*(1), 10-14.

Franceschi-Bicchierai, L. (2016, September 30). *How 1.5 million connected cameras were hijacked to make an unprecedented botnet*. Motherboard. https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs

Franklin, T. R., & Sutton, M. (2009). Third-party coverage. In *Cyber Liability and Insurance: Managing the Risks of Intangible Assets* (pp. 89-124). National Underwriter Company.

Frei, J. (2020, September). *Israel's national cybersecurity and cyberdefense posture.* Center for Security Studies. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

Fruhlinger, J. (2017, August 22). *What is Stuxnet, who created it and how does it work?* CSO Australia: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Fulford, M. (2020, February 24). *6 essential steps for an effective cybersecurity risk assessment*. LBMC. https://www.lbmc.com/blog/effective-cybersecurity-risk-assessment/

Galletta, A., & Cross, W. (2013). *Mastering the semi-structured interview and beyond: From research design to analysis and publication.* NYU Press.

Galvin, R. (2015). How many interviews are enough? Do qualitative interviews in building energy consumption research produce reliable knowledge? *Journal of Building Engineering*, 1, 2–12. https://doi.org/10.1016/j.jobe.2014.12.001

Garger, J. (2020, January 29). *Determine readability using the Flesch reading ease*. https://www.johngarger.com/blog/determine-readability-using-the-flesch-reading-ease

Gekara, V., Snell, D., Molla, A., Karanasios, S., & Thomas, A. (2019). *Skilling the Australian workforce.* National Centre for Vocational Education Research (NCVER). https://www.ncver.edu.au/__data/assets/pdf_file/0026/5744123/Skilling-the-Australian-workforce-for-the-digital-economy.pdf

Gendreau, A. (2016). Internet of Things: Arduino vulnerability analysis. *ISSA Journal, August*, 32-47.

George Mason University. (2018). *How to write a research question*. The Writing Center. https://writingcenter.gmu.edu/guides/how-to-write-a-research-question

Ghoshal, A. (2018, March 2). *How GitHub braved the world's largest DDoS attack*. The Next Web. https://thenextweb.com/security/2018/03/02/how-github-braved-the-worlds-largest-ddos-attack/

GIAC. (2021, December 9). *Get certified*. https://www.giac.org/get-certified/?msc=main-nav

Gilfillan, G. (2015, December 1). *Definitions and data sources for small business in Australia: A quick guide*. Parliament of Australia. https://www.aph.gov.au/about_parliament/parliamentary_departments/parliamentary_library/pubs/rp/rp1516/quick_guides/data

GitHub. (2018, October 1). *The state of the octoverse*. Octoverse-GitHub. https://octoverse.github.com/2018/

Goedde, A. (2021). *State of the internet: A year in review*. Akamai https://www.akamai.com/content/dam/site/en/documents/state-of-the-internet/soti-security-a-year-in-review-report-2020.pdf

Goleman, D. (2015, August 1). *What's the difference between creativity and innovation?* World Economic Forum. https://www.weforum.org/agenda/2015/01/whats-the-difference-between-creativity-and-innovation/

Goodin, D. (2016, September 29). *Record-breaking DDoS reportedly delivered by >145k hacked cameras*. Ars Technica. https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

Goodman, S. (2020, February 7). *Human error to blame for 9 in 10 UK cyber data breaches in 2019*. CYBSafe. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

Google. (2019, April). *Google cloud platform: Shared responsibility matrix.* https://services.google.com/fh/files/misc/gcp_pci_srm__apr_2019.pdf

Gopalan, V. (2019, July 18). *Application layer 7 DDoS attacks*. Indusface. https://www.indusface.com/blog/application-layer-7-ddos-attacks/

Gould, J. (2016). What's the point of the PhD thesis? *Nature, 535,* 26-28 https://www.nature.com/news/what-s-the-point-of-the-phd-thesis-1.20203

Graham, R. (2015, April 1). *Pin-pointing China's attack against GitHub*. Errata Security. https://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html#.Xh_pb1MzbUK

Green, C. H. (2019, August 12). *The dark art of ghosting in business*. Trusted Advisor. https://trustedadvisor.com/trustmatters/the-dark-art-of-ghosting-in-business

Griffith, K. (2016, August 3). *New study: Companies might be suppressing employee opinions when they need them the most* [Blog]. University of Denver. https://daniels.du.edu/blog/new-study-companies-might-be-suppressing-employee-opinions-when-they-need-them-the-most/

Grim, J., Thapar, A., Ayera, A., Sharma, A., Villatta, N., Werts, D. J., & Alvarez-Fernandez, D. J. (2020). *Cyber-espionage-report.* Verizon. https://www.verizon.com/business/resources/reports/2020-2021-cyber-espionage-report.pdfx

Grimes, R. A. (2007, November 3). *Don't laugh at Estonia -- it could happen to you*. CSO Australia. https://www.csoonline.com/article/2633116/don-t-laugh-at-estonia----it-could-happen-to-you.html

Groves, R. (2021). *DDoS attack mitigation*. A10 Networks. https://www.a10networks.com/wp-content/uploads/A10-EB-ddos-attack-mitigation-a-threat-intelligence-report.pdf

Gutnikov, A., Badovskaya, E., Kupreev, O., & Shmelev, Y. (2021, July 28). *DDoS attacks in Q2 2021*. Secure List. https://securelist.com/ddos-attacks-in-q2-2021/103424/

Gutnikov, A., Kupreev, O., & Shmelev, Y. (2021, November 8). *DDoS attacks in Q3 2021*. Securelist. https://securelist.com/ddos-attacks-in-q3-2021/104796/

Hamann, F. (2019, December 3). *Have you been 'ghosted' in business? Here's how to tell*. Flying Solo. https://www.flyingsolo.com.au/uncategorized/have-you-been-ghosted-in-business-heres-how-to-tell/

Harper, L., Kalfa, N., Beckers, G., Kaefer, M., Nieuwhof-Leppink, A. J., Fossum, M., & Herbst, K. W. (2020). The impact of COVID-19 on research. *Journal of Pediatric Urology*, *16*(5), 715-716. https://doi.org/10.1016/j.jpurol.2020.07.002

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review*, *40*(2), 265-281. https://doi.org/10.1108/OIR-04-2015-0106

Hatfield, J. M. (2018). The evolution of a concept. Computers & Security. *Social engineering in cybersecurity*, *73*, 102-103. https://doi.org/10.1016/j.cose.2017.10.008

Hawkins, P. (2020, October). *Australian Government revenue*. Parliament of Australia.

https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview202021/AustralianGovernmentRevenue#:~:text=Revenue%20is%20forecast%20to%20decline,the%20economy%20since%202011%E2%80%9312.

Heard, S. B. (2016). *The canonical structure of the scientific paper.* Princeton University Press. https://doi.org/10.2307/j.ctvcmxs67.12

Heimdal Security. (2020, March 2). *Challenges in software security for IoT devices (and how to tackle them).* https://heimdalsecurity.com/blog/challenges-security-for-iot/

Helms, M. M., & Nixon, J. (2010). Exploring SWOT analysis - where are we now?: A review of academic research from the last decade. *Journal of Strategy and Management, 3*(3), 215-251. https://doi.org/10.1108/17554251011064837

Hendry, J. (2021, June 9). *Govt to mandate essential eight cyber security controls*. IT News. https://www.itnews.com.au/news/govt-to-mandate-the-essential-eight-cyber-security-controls-565699

Henshel, D. S. (2016). *Integrating cultural factors into human factors framework for cyber attackers* [Paper presentation]. Seventh Annual Conference on Applied Human Factors and Ergonomics Conference, Orlando, Florida. https://link.springer.com/chapter/10.1007/978-3-319-41932-9_11

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Holistic Cyber Security Risk Assessment. Procedia Manufacturing, 3*, 1117-1124. https://doi.org/10.1016/j.promfg.2015.07.186

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herpig, S. (2015). *Anti-war and the cyber triangle : Strategic implications of cyber operations and cyber security for the state* [PhD thesis, Unversity of Hull]. ProQuest Dissertations & Theses Global.

Hofstead, G., Hofstead, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind.* McGraw Hill.

Hogue, R. J. (2011, November 17). *Axiology – What do you value in research?*[Blog] https://rjhogue.name/2011/11/17/axiology-what-do-you-value-in-research/

Holmes, O. (2018, March 21). *Israel confirms it carried out 2007 airstrike on Syrian nuclear reactor*. The Guardian. https://www.theguardian.com/world/2018/mar/21/israel-admits-it-carried-out-2007-airstrike-on-syrian-nuclear-reactor

Hounshell, B. (2007, October 5). *Syrian radar p0wned by Israeli military hackers?* Foreign Policy. https://foreignpolicy.com/2007/10/05/syrian-radar-p0wned-by-israeli-military-hackers/

Hox, J. J., & Boeije, H. R. (2005). Data collection, primary versus secondary. In K. Kempf-Leonard (Ed.), *Encyclopedia of social measurement* (pp. 593-599). Elsevier.

Hua, Z. (2016). *Research methods in intercultural communication : A practical guide.* Wiley Blackwell.

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology, 29*(3), 221-232.

Hulme, G. V. (2019, February 21). *DDoS explained: How distributed denial of service attacks are evolving*. CSO Australia. https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html

Humphrey, A. S. (2005). SWOT Analysis for management consulting. *SRI Alumni Association Newsletter, December*, 7-8. https://web.archive.org/web/20130104102543/http://www.sri.com/sites/default/files/brochures/dec-05.pdf

Hunker, J. (2010, November). *Cyber war and cyber power. Issues for NATO doctrine.* Nato Defense College. http://www.ndc.nato.int/download/downloads.php?icode=230

Huntsman. (2019, January 21). *Cyber crime is a growing industry*. https://www.huntsmansecurity.com/blog/cyber-crime-is-a-growing-industry/

Internet Assigned Numbers Authority. (2018, June 15). *Internet Control Message Protocol (ICMP) parameters*. IANA. https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

Internet Assigned Numbers Authority. (2020, January 17). *Service name and transport protocol port number registry*. IANA. https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Ibrahim, H., Islam, K., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6). https://doi.org/10.3390/app8060898

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Imperva. (2018, December). *What is an NTP amplification attack*. https://www.imperva.com/learn/application-security/ntp-amplification/

Imperva. (2021). *2021 DDoS threat landscape report*. https://www.imperva.com/resources/resource-library/reports/ddos-threat-landscape-report/

Incapsula. (2016, September 30). *Global DDoS threat landscape Q3 2016*. https://www.incapsula.com/ddos-report/ddos-report-q3-2016.html

Incapsula. (2017a, September 30). *Global DDOS threat landscape Q3 2017*. https://www.incapsula.com/ddos-report/ddos-report-q3-2017.html

Incapsula. (2017b, March 31). *Global DDoS threat landscape Q1 2017*. https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html

Internet World Stats. (2019, November 11). *Internet growth statistics*. https://www.internetworldstats.com/emarketing.htm

Irwin, L. (2021, Aug 19). *The cyber security risks of working from home*. IT Governance. https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home

ISACA. (2021, November 16). *Credentialing*. https://www.isaca.org/credentialing

ISO. (2021). *ISO/IEC 27001: Information security management*. https://www.iso.org/isoiec-27001-information-security.html

Jackson, B. (2019, October 6). *How to stop a DDoS attack in its tracks (case study)*. Kinsta. https://kinsta.com/blog/ddos-attack/

Jackson, J. (2021, January). *How much will a DDoS attack cost yourbusiness?* Cloudbric. https://www.cloudbric.com/blog/2021/01/business-ddos-attacks-damages-and-cost/

Janczewski, L. J., & Colarik, A. M. (2008). *Cyber warfare and cyber terrorism, information science reference.* IGI Global.

Jeftovic, M. E. (2016, October 24). *The DNS attack: What it means, "who did it?" and how to deal*. Easy DNS. https://easydns.com/blog/2016/10/24/the-dns-attack-what-it-means-who-did-it-and-how-to-deal/

Jenkins, Q. (2014, July 7). *Second arrest in response to DDoS attack on Spamhaus*. Spamhaus. https://www.spamhaus.org/news/article/715/second-arrest-in-response-to-ddos-attack-on-spamhaus

Jing, H., & Wang, J. (2020). DDoS detection based on graph structure features and non-negative matrix factorization. *Concurrency and Computation Practice and Experience, 34*(9) https://doi.org/10.1002/cpe.5783

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to cyber threat information sharing.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-150

Johnston, A. C., Wech, B. A., Jack, E. P., & Beavers, M. (2010). *Reigning in the remote employee: Applying social learning theory to explain information security policy compliance attitudes*. Sustainable IT Collaboration Around the Globe: 16th Americas Conference on Information Systems (p. 493). AMCIS.

Johnston, I. (2020). Australia's public health response to COVID-19: What have we done, and where to from here? *Australian and New Zealand Journal of Public Health, 44*(6), 440-445. https://doi.org/10.1111/1753-6405.13051

Johnston, M. P. (2017). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries, 3*(3), 619-626.

Joint Task Force. (2018, December). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy.* NIST. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Jones, S. (2015, September 24). *PLATO computer-based education system*. Encylopedia Britannica. https://www.britannica.com/topic/PLATO-education-system

J. P. Morgan (2021). How criminals use social engineering to target your company *Fraud + Cybersecurity*. https://www.jpmorgan.com/content/dam/jpm/commercial-banking/insights/cybersecurity/899213-summer-21-fraud-cyber-mag_full-issue-final-ada-071221.pdf

Jovic, D. (2020, November 20). *The future is now – 37 fascinating chatbotsStatistics.* Small Biz Genius. https://www.smallbizgenius.net/by-the-numbers/chatbot-statistics/

Jupp, V. (2006). Documents and critical research. In V. Jupp, R. Sapsford, & V. Jupp (Eds.), *Data collection and analysis* (pp. 272-289). Sage Publications Ltd. https://doi.org/10.4135/9781849208802.n12

Kabachinski, J. (2015). The OSI reference model: Part of the networking vernacular. *24x7*, *20*(2), 20.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kandasamy, K., Srinivas, S., Achuthan, K., & Ragan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security, 8*. https://doi.org/10.1186/s13635-020-00111-0

Kang, C. (2016, June 14). Court backs rules treating internet as utility, not luxury. *New York Times*. https://www.nytimes.com/2016/06/15/technology/net-neutrality-fcc-appeals-court-ruling.html

Kang, S.-H., Park, K.-Y., Yoo, S.-G., & Kim, J. (2013). DDoS avoidance strategy for service availability. *Cluster Computing: The Journal of Networks, Software Tools and Applications*, *16*(2), 241-248.

Kara, H., & Khoo, S.-M. (2020, October 26). *How the pandemic has transformed research methods and ethics: 3 lessons from 33 rapid responses* [Blog]. London School of Economics. https://blogs.lse.ac.uk/impactofsocialsciences/2020/10/26/how-the-pandemic-has-transformed-research-methods-and-ethics-3-lessons-from-33-rapid-responses/

Karahanna, E., Evaristo, J. R., & Srite, M. (2005). Levels of culture and individual behavior: An investigative perspective. *Journal of Global Information Management (JGIM), 13*(2), 1-20.

Kaspersky. (2021, November 8). *DDoS attacks in Q3 grow by 24%, become more sophisticated*. https://www.kaspersky.com/about/press-releases/2021_ddos-attacks-in-q3-grow-by-24-become-more-sophisticated

Kaspersky, E. (2016, December 6). *A brief history of DDoS attacks.* https://eugene.kaspersky.com/2016/12/06/a-brief-history-of-ddos-attacks/

Kazerooni, S. (2015). State of denial: Casinos have a lot to learn when it comes to detecting and preventing costly DDoS attacks. *Casino Journal, 28*(1), 40.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computer and Security, 61*, 46-58. https://doi.org/10.1016/j.cose.2016.05.006

Kenton, W. (2019, May 20). *Economies of scale*. Investopedia. https://www.investopedia.com/terms/e/economiesofscale.asp

Kerner, S. M. (2019, February 1). *Why Amazon's AWS cloud business will continue to grow*. eWeek. https://www.eweek.com/cloud/why-amazon-s-aws-cloud-business-will-continue-to-grow

Khalili, J. (2022, January). *Kids won't stop launching DDoS attacks against their schools*. Techradar. https://www.techradar.com/news/kids-wont-stop-launching-ddos-attacks-against-their-schools

Khalimonenko, A., & Kupreev, O. (2017, May 11). *DDOS attacks in Q1 2017*. SecureList https://securelist.com/ddos-attacks-in-q1-2017/78285/

Khalimonenko, A., Kupreev, O., & Ilgan, K. (2017, November 6). *DDoS attacks in Q3 2017*. Securelist https://securelist.com/ddos-attacks-in-q3-2017/83041/

Khalimonenko, A., Kupreev, O., & Badovskaya, E. (2018, April 26). *DDoS attacks in Q1 2018*. SecureList. https://securelist.com/ddos-report-in-q1-2018/85373/

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly cyber security threats amid COVID-19 pandemic.* Taylors University. https://seap.taylors.edu.my/file/rems/publication/109566_7215_1.pdf

Kiley, M., Holbrook, A., Lovat, T., Fairbairn, H., Starfield, S., & Paltridge, B. (2018, February 6). *An oral component in PhD examination in Australia: Issues and considerations (AUR 60 01)*. National Tertiary Education Union. https://www.nteu.org.au/unda/article/An-oral-component-in-PhD-examination-in-Australia%3A-Issues-and-considerations-%28AUR-60-01%29-20307

Kiyuna, A., & Conyers, L. (2015). *Cyberwarefare sourcebook.* Lulu.com.

Kizza, J. M. (2017). *Guide to computer network security.* Springer International Publishing.

Koepke, P. (2017, June). *Cybersecurity information sharing incentives and barriers.* Massachusetts Institute of Technology. http://web.mit.edu/smadnick/www/wp/2017-13.pdf

Kolenko, M. M. (2019). *Cyber defender cultural patterns and operational behavior* [Doctor of Science dissertation, Capitol Technology University]. ProQuest Dissertations Publishing, 27547553.

Koomey, J., Berard, S., Sanchez, M., & Wong, H. (2011, Mar). Implications of historical trends in the electrical efficiency of computing. *IEEE Annals of the History of Computing, 33*(3), 46-54.

Korolov, M. (2017, September 27). *Why DDoS attacks are on the rise*. Data Center Knowledge. https://www.datacenterknowledge.com/security/why-ddos-attacks-are-rise

Kost, E. (2022, March 4). *11 biggest data breaches in Australia (includes 2021 attacks)*. Upguard. https://www.upguard.com/blog/biggest-data-breaches-australia

Kotler, P., Burton, S., Deans, K., Brown, L., & Armstrong, G. (2013). *Marketing* (9th ed.). Pearson Australia Group Pty Ltd.

Kottler, S. (2018, March 1). *February 28th DDoS incident report*. GitHub. https://github.blog/2018-03-01-ddos-incident-report/

Kovacs, E. (2022, January 27). *Microsoft saw record-breaking DDoS attacks exceeding 3 Tbps*. Security Week. https://www.securityweek.com/microsoft-saw-record-breaking-ddos-attacks-exceeding-3-tbps

KPMG. (2020, November 6). *Cyber security in the new reality*. https://home.kpmg/xx/en/home/insights/2020/04/the-cyber-security-implications-of-covid-19.html

Krebs, B. (2013, April 26). *Dutchman arrested in Spamhaus DDoS*. Krebs on Security. https://krebsonsecurity.com/2013/04/dutchman-arrested-in-spamhaus-ddos/

Krebs, B. (2016, October 21). *DDoS on Dyn impacts Twitter, Spotify, Reddit*. Krebs on Security. https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

Krebs, B. (2019, February 1). *250 webstresser users to face legal action*. Krebs on Security. https://krebsonsecurity.com/2019/02/250-webstresser-users-to-face-legal-action/

Kuhn, T. S. (1970). *The structure of scientific revolutions* (3rd ed.). University of Chicago Press. https://ia601209.us.archive.org/9/items/ThomasS.KuhnTheStructureOfScient

ificRevolutions/Thomas_S._Kuhn_The_structure_of_scientific_revolutions.pdf

Kupreev, O., Badovskaya, E., & Gutnikov, A. (2018, October 31). *DDoS attacks in Q3 2018*. SecureList. https://securelist.com/ddos-report-in-q3-2018/88617/

Kupreev, O., Badovskaya, E., & Gutnikov, A. (2019a, May 21). *DDoS attacks in Q1 2019*. SecureList. https://securelist.com/ddos-report-q1-2019/90792/

Kupreev, O., Badovskaya, E., & Gutnikov, A. (2019b, August 5). *DDoS attacks in Q2 2019*. SecureList. https://securelist.com/ddos-report-q2-2019/91934/

Kupreev, O., Badovskaya, E., & Gutnikov, A. (2019c, November 11). *DDoS attacks in Q3 2019*. SecureList. https://securelist.com/ddos-report-q3-2019/94958/

Kupreev, O., Strohschneider, J., & Khali, A. (2016, October 31). *Kaspersky DDOS intelligence report for Q3 2016*. SecureList. https://securelist.com/kaspersky-ddos-intelligence-report-for-q3-2016/76464/

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Lanfear, T., & Berry, D. (2022, January 3). *Shared responsibility in the cloud*. Microsoft. https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

LaQuey, T. L. (Ed.) (1990). *The user's directory of computer networks.* Elsevier. https://www.sciencedirect.com/book/9781555580476/the-users-directory-of-computer-networks

Lavino, J. G., & Neumann, R. B. (2010). *Psychology of risk perception.* Nova Science Publishers, Inc.

Leiner, B. M., Cerf, V. G., Clarke, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L., & Wolff, S. (1997). *A brief history of the internet*. Internet Society. http://www.isoc.org/internet/history/brief.shtml

Lewis, J. (2020, April 9). *Covid-19 insights - Emerging risks*. KPMG. https://home.kpmg/xx/en/home/insights/2020/04/covid-19-insights-emerging-risks.html

Li, Q., & Schaub, D. (2004). Economic globalization and transnational terrorism: A pooled time-series analysis. *Journal of Conflict Resolution, 48*(2), 230-258.

Li, R. (2016, November 8). *How to leverage baidu analytics to grow your digital presence in China*. KoMArketing. https://komarketing.com/blog/leverage-baidu-analytics-to-grow-your-digital-presence-in-china/

Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge University Press.

Libicki, M. C. (2009). *Cyber deterrence and cyberwar*. Rand. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.sum.pdf

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry.* Sage Publications.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security studies, 22*(3), 365-404. https://doi.org/10.1080/09636412.2013.816122

Lindsey, N. (2019, April 16). *Iranian hackers increasing their activity worldwide as part of new cyber-espionage program*. CPO. https://www.cpomagazine.com/cyber-security/iranian-hackers-increasing-their-activity-worldwide-as-part-of-new-cyber-espionage-program/

Lonsdale, D. (2004). *The nature of war in the information age. A Clausewitzian future.* Frank Class.

Lord, B. (2016, September 22). *An important message about Yahoo user security*. Tumblr https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security

MacDonald, K., & Tipton, C. (1993). Using documents. In N. Gilbert (Ed.), *Researching social life* (pp. 28-52). Sage.

Madhra, S. (2017, February 11). *Management vs staying technical*. LinkedIn. https://www.linkedin.com/pulse/management-vs-staying-technical-suresh-madhra/

Mallon, T., & Kirsch, A. (2014, June 24). When we read fiction, how relevant is the author's biography? *The New York Times*. https://www.nytimes.com/2014/06/29/books/review/when-we-read-fiction-how-relevant-is-the-authors-biography.html

Mansfield-Devine, S. (2015). The growth and evolution of DDoS. *Network Security, 2015*(10), 13-20.

Manuel, J. (2018, April 16). *Searching for the reuse of Mirai code: Hide 'N Seek Bot*. Fortinet. https://www.fortinet.com/blog/threat-research/searching-for-the-reuse-of-mirai-code--hide--n-seek-bot.html

Marczak, B., & Scott-Railton, J. (2020). *Move fast and roll your own crypto: A quick look at the confidentiality of Zoom meetings.* The Citizen Lab. https://citizenlab.ca/2020/04/movefast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoommeetings/

Marriott, J. W. (2011, March 30). *Gartner*. Gartner. https://www.gartner.com/imagesrv/summits/docs/na/customer-360/C360_2011_brochure_FINAL.pdf

Marrison, C. (2015). Understanding the threats to DNS and how to secure it. *Network Security, 2015*(10), 8-10.

Marshall, M. G., Gurr, T. R., & Jaggers, K. (2019, Jun 27). *Polity v project.* Systemic Peace. http://www.systemicpeace.org/inscr/p4manualv2018.pdf

Mattick, K., Johnston, J., & de la Croix, A. (2018). How to write a good research question. *The Clinical Teacher, 15*(2), 104-108. https://doi.org/10.1111/tct.12776

Mauslein, J. A. (2014). *Three essays on international cyber threats: Target nation characteristics, international rivalry, and asymmetric information exchange* [PhD thesis, Kansas State University]. ProQuest Dissertations & Theses Global.

Maxwell, J. A. (1992). Understanding and validity in qualitative research. *Harvard Educational Review, 62*(3), 279-300.

Maxwell, J. A. (2012). *Qualitative research design: An interactive approach.* Sage Publications.

McClelland, D. C. (2010). *The achieving society.* Martino Fine Books.

McClure, S., & Scambray, J. (1999). Don't forget those unguarded modem lines when assessing your security risks. *Infoworld, 21*(2), 77.

McFarlane, R. (2017, July 6). *The growing danger of IP theft and cyber extortion.* Dark Reading. https://www.darkreading.com/cloud/the-growing-danger-of-ip-theft-and-cyber-extortion/a/d-id/1329247

McGuinness, D. (2017, April 27). *How a cyber attack transformed Estonia*. BBC. http://www.bbc.com/news/39655415

McKeay, M. (2017, November 14). *State of the internet security report Q3 2017.* Akamai. https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q3-2017-state-of-the-internet-security-report.pdf

McKee, L. (2021, January 21). *Am I legally required to have a privacy policy for my business.* . Legal Vision. https://legalvision.com.au/am-i-legally-required-to-have-a-privacy-policy/

Meade, M. J., & Dreyer, C. W. (2020). Orthodontic temporary anchorage devices: A qualitative evaluation of internet information available to the general public. *American Journal of Orthodontics and Dentofacial Orthopedics, 158*(4), 612-620.

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative research : A guide to design and implementation.* John Wiley & Sons, Incorporated.

Messmer, E. (1999, May 12). *Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says*. CNN. http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/

Metcalf, R. (2020, February 27). Pipeline attack highlights cybersecurity risk to energy infra. *Power Finance & Risk*.

Microsoft Corporation. (2021). *Microsoft Excel*. https://www.microsoft.com/en-au/microsoft-365/excel

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (*2*nd ed.).. Sage. https://vivauniversity.files.wordpress.com/2013/11/milesandhuberman1994.pdf

Miller, M. (2020, March 3). *Hackers find new target as Americans work from home during outbreak*. The Hill. https://thehill.com/policy/cybersecurity/487542-hackers-find-new-target-as-americans-work-from-home-during-outbreak

Miller, R. (2019, Feb 2). *AWS and Microsoft reap most of the benefits of expanding cloud market*. Techcrunch. https://techcrunch.com/2019/02/01/aws-and-microsoft-reap-most-of-the-benefits-of-expanding-cloud-market/

Millman, R. (2017, November 21). *DDoS attacks almost double with IoT as target, says Corero*. Internet of Business. https://internetofbusiness.com/ddos-attacks-double-iot-target-corero/

Mills, J., & Harmon-Jones, E. (1999). *Cognitive dissonance : progress on a pivital theory in social psychology* (1st ed., Ser. Apa science volumes). American Psychological Association.

Minei, E., & Matusitz, J. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. *Journal of Human Behavior in the Social Environment, 21*(8), 995-1019. https://doi.org/10.1080/10911359.2011.588569

Ministers for the Department of Industry, Science, Energy and Resources. (2018, Apr 5). *Cooperative research centre to strengthen cyber security.* https://www.minister.industry.gov.au/ministers/cash/media-releases/cooperative-research-centre-strengthen-cyber-security

Monash University. (2020, November 20). *World's fastest internet speed from a single optical chip*. Science Daily. https://www.sciencedaily.com/releases/2020/05/200522095504.htm

Monowar, B. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters, 51*(1).

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics, 38*(8), 82-85.

Moses, A. (2013, February 18). Rise in cyber attacks on Australian businesses. *The Sydney Morning Herald*. https://www.smh.com.au/technology/rise-in-cyber-attacks-on-australian-businesses-20130218-2em94.html

Mossburg, E., Gelinne, J., & Calzada, H. (2016, June). *Beneath the surface of a cyberattack: A deeper look at business impacts.* Deloitte. https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

Munawar, H. S., Khan, S. I., Ullah, F., Kouzani, A. Z., & Mahmud, M. A. (2021). Effects of COVID-19 on the Australian economy: Insights into. *Sustainability, 13*(20), 11300.

Murray, A. (2009). *Prince2 : Managing successful projects with Prince2.* The Stationary Office.

National Academies of Sciences, Engineering, and Medicine. (2019). *Reproducibility and replicability in science.* National Academies Press.

Nazario, J. (2008). DDoS attack evolution[Report]. *Network Security, 2008*(7), 7.

Neset, S. (2018, June 4). *Cognitive psychology concepts for understanding corrupt behaviour* CMI U4 - Anti Corruption Resource Centre. https://www.u4.no/cognitive-psychology-concepts-for-understanding-corrupt-behaviour

Netscout. (2018). *13th annual worldwide infrastructure security report.* https://resources.netscout.com/threat-report-archives/13th-worldwide-infrastructure-security-report

Netscout. (2019). *14th annual worldwide infrastructure security report.* https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901%E2%80%93WISR.pdf

Netscout. (2021a). *Netscout threat intelligence report: Findings from 1H 2021*. https://www.netscout.com/sites/default/files/2021-09/ThreatReport_1H2021_FINAL.pdf

NetScout. (2021b). *Netscout Threat Intelligence Report*: *Findings from second half 2021* https://www.netscout.com/threatreport/

Neuman, W. L. (2006). *Social research methods: Qualitative and quantitative approaches* (6th ed.). Pearson/AandB.

Newbury, D. (2016, December 11). *The entire internet 1973.* Twitter. https://twitter.com/workergnome/status/807704855276122114/photo/1

Newman, S. (2021, October 17). *The true cost of DDoS attacks*. Info Security. https://www.infosecurity-magazine.com/opinions/the-true-cost-of-ddos-attacks/

National Health and Medical Research Council, & Australian Research Council. (2018). *National statement on ethical conduct in human research (2007) - Updated 2018.* NHMRC. https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018#toc__235

Nichols, S. (2019, September 5). *Newb admits he ran Satori botnet that turned thousands of hacked devices into a 100Gbps+ DDoS-for-hire cannon*. The Register. https://www.theregister.co.uk/2019/09/05/satori_plea_deal/

Nicholson, P. (2020, June 24). *AWS hit by largest reported DDoS attack of 2.3 Tbps*. A10. https://www.a10networks.com/blog/aws-hit-by-largest-reported-ddos-attack-of-2-3-tbps/

Nicholson, P. (2022, January 21). *Five most famous DDoS attacks and then some*. A10. https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Nisbett, R. E., Peng, K., Choi, I., & Norenzayan, A. (2001). Culture and systems of thought: Holistic versus analytic cognition. *Psychological Review, 108*(2), 291-310. https://doi.org/10.1037//0033-295X.108.2.291

Norsar. (2016, June 30). *Arpanet.* https://www.norsar.no/about-us/history/arpanet-article774-270.html

Novinson, M. (2018, September 11). *8 biggest DDoS attacks today and what you can learn from them*. CRN. https://www.crn.com/slide-shows/security/8-biggest-ddos-attacks-today-and-what-you-can-learn-from-them

Nweke, L. O., & Wolthusen, S. (2020). *Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection*. 12th International Conference on Cyber Conflict (CyCon) (pp. 63-78). IEEE. http://doi.org/10.23919/CyCon49761.2020.9131721

Nyman, J. (2018). *Evaluating the mitigating effect on HTTP flood attacks using an application layer challenge-response approach* [Unpublished master's thesis]. Umea Universitet. https://www.diva-portal.org/smash/get/diva2:1223901/FULLTEXT01.pdf

Office of the Australian Information Commissioner. (2021a). *What is a privacy policy?* https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-a-privacy-policy/

Office of the Australian Information Commissioner. (2021b). *Report a data breach*. https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/

O'Donnell, A. (2016, June 20). *It's official—High-speed internet is considered a utility*. Odyssey. https://www.theodysseyonline.com/high-speed-internet-considered-utility

Of Cables and Conspiracies. (2008, February 7). *The Economist*. https://www.economist.com/international/2008/02/07/of-cables-and-conspiracies

Offensive Security. (2021, December). *Courses and certifications*. https://www.offensive-security.com/courses-and-certifications/

Omer, S. K. (2018). SWOT analysis: The tool of organizations stability (KFC) as a case study. *Journal of Process Management. New Technologies, 6*(4), 27-34. https://doi.org/10.5937/jouproman6-19188

Oppewal, H. (2010). *Wiley international encyclopedia of marketing: Causal research.* Wiley International. https://doi.org/10.1002/9781444316568.wiem02001

Optus. (2022). *Home internet*. Optus. https://www.optus.com.au/broadband-nbn/home-broadband/plans/shop

Orlowski, A. (2016, September 12). *Meet DDoSaaS: Distributed denial of service-as-a-service*. The Register. https://www.theregister.co.uk/2016/09/12/denial_of_service_as_a_service/

Ostiguy, P. (2021, February 16). *The distributed workforce is here to stay - Here's why performance matters*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/02/16/the-distributed-workforce-is-here-to-stayheres-why-performance-matters/?sh=4db2116e317c

OwnCloud. (2020, April 3). *Collaborate easier, safely*. https://owncloud.org/

Palmer, D. (2016, September 2). *Cybercrime Inc: How hacking gangs are modeling themselves on big business*. ZDNet. https://www.zdnet.com/article/cybercrime-inc-how-hacking-gangs-are-modeling-themselves-on-big-business/

Palmer, D. (2020, February 25). *IoT security fail: The weird devices that employees are connecting to the office network.* ZDNet. https://www.zdnet.com/article/iot-security-warning-employees-are-connecting-these-unauthorised-devices-to-your-network/

Palmquist, M., & Connor, P. (2012). *What are the author's biases?* Writing @ CSU. https://writing.colostate.edu/guides/page.cfm?pageid=226&guideid=15

Patterson, J. (2016, May 11). *How long does it take to do a PhD*. The Thesis Whisperer. https://thesiswhisperer.com/2016/05/11/how-long-does-it-take-to-do-a-phd/

Paul, K. (2020, December 24). *Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs*. The Guardian. https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats

Pauli, D. (2017, March 10). *Cybersecurity: Island Australia collapses.* The Mandarin. https://www.themandarin.com.au/76634-cybersecurity-island-australia-collapses/

Pham, L. (2018). *Review of key paradigms: Positivism, interpretivism and critical inquiry*. https://doi.org/10.13140/RG.2.2.13995.54569.

Pinker, S. (2018, February 17). *The media exaggerates negative news. This distortion has consequences*. The Guardian. https://www.theguardian.com/commentisfree/2018/feb/17/steven-pinker-media-negative-news

Pitlik, D. (2019, July 1). *DDoS attacks growing ever-more sophisticated and efficient*. NetScout. https://www.netscout.com/blog/ddos-attacks-growing-ever-more-sophisticated-and-efficient

Project Management Institute. (2013). *A guide to the project management body of knowledge (PMBoK guide)* (5th ed.).

Porter, J. (2019, June 13). *Telegram blames China for 'powerful DDoS attack' during Hong Kong protests*. The Verge. https://www.theverge.com/2019/6/13/18677282/telegram-ddos-attack-china-hong-kong-protest-pavel-durov-state-actor-sized-cyberattack

Pranggono, B., & Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters, 4*(2), 1-6. https://doi.org/10.1002/itl2.247

Priceonomics Data Studio. (2019, January 9). *The IoT data explosion: How big is the IoT data market?* https://priceonomics.com/the-iot-data-explosion-how-big-is-the-iot-data/

PricewaterhouseCoopers. (2020, March). *Managing the impact of COVID-19 on cyber security*. https://www.pwccn.com/en/issues/cybersecurity-and-privacy/covid-19-impact-mar2020.html

Punch, K. F. (2016). *Social research: Quantitative & aualitative approaches.* Sage Publications Ltd.

QSR International. (2021). *NVivo 12*. https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/support-services/nvivo-downloads

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting and Management, 8*(3), 238-264.

Queensland Health. (2020). *Department of Health media releases*. https://www.health.qld.gov.au/news-events/doh-media-releases

Quinn, J. B. (1967, March). *Technological forecasting*. Retrieved from Harvard Business Review. https://hbr.org/1967/03/technological-forecasting

Radware. (2017, March 13). *History of DDoS attacks*. https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/

Radware. (2021). *Quarterly DDoS and application attack report*. https://www.radware.com/2021q3-ddos-report/

Raj, M. (2018). *Python penetration testing essentials: Techniques for ethical hacking with python* (2nd ed.). Packt Publishing Limited.

Rajamäki, J. (2019). *D3.6 ECHO information sharing models*. European Commission. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c8e7ae90&appId=PPGMS

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest. *IOP Conference Series. Materials Science and Engineering, 981*(2). https://doi.org/10.1088/1757-899X/981/2/022062

Ramos, S. (2021, March 1). *COVID-19's impact felt by researchers*. American Psychological Association. https://www.apa.org/science/leadership/students/covid-19-impact-researchers

Rao, U. H., & Nayak, U. (2014). Rao, U. H., & Nayak, U. (2014). *The InfoSec handbook: An introduction to information security*. Apress. https://doi.org/10.1007/978-1-4302-6383-8.

Ramprasath, J., & Seethalakshmi, V. (2021). Improved network monitoring using software-defined networking for DDoS detection and mitigation evaluation. *Wireless Personal Communication, 116*(3), 2743-2757. https://doi.org/10.1007/s11277-020-08042-2

Rastogi, N., & Trivedi, M. K. (2016). PESTLE technique – A tool to identify external risks in construction projects. *International Research Journal of Engineering and Technology, 3*(01), 384-388. https://www.irjet.net/archives/V3/i1/IRJET-V3I165.pdf

Rayome, A. D. (2017, November 20). *DDoS attacks increased 91% in 2017 thanks to IoT*. Techrepublic. https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/

Rayome, A. D. (2019, May 21). *Massive DDoS attacks lasting more than an hour increased 487% in 2019*. Tech Republic. https://www.techrepublic.com/article/massive-ddos-attacks-lasting-more-than-an-hour-increased-487-in-2019/

Reason, J. (2000). Human error: Models and management. *BMJ, 320*(7237), 768-770. https://doi.org/10.1136/bmj.320.7237.768

Red Canary. (2021). *2021 threat detection report*. https://redcanary.com/threat-detection-report/

Remeikis, A. (2019, February 8). *Australian security services investigate attempted cyber attack on parliament.* The Guardian. https://www.theguardian.com/australia-news/2019/feb/08/asio-australian-

security-services-hack-data-breach-investigate-attempted-cyber-attack-parliament

Reuters. (2014, July 5). *Israel's high tech boom threatened by shallow labor pool.* YNetNews. http://www.ynetnews.com/articles/0,7340,L-4824677,00.html

Reuters. (2015, June 25). *Australian company devastated by Chinese hacking, IP theft*. CRN. https://www.crn.com.au/news/australian-company-devastated-by-chinese-hacking-ip-theft-405725

Rewhorn, S. (2018). Writing your successful literature review. *Journal of Geography in Higher Education , 42*(1), 143-147.

Rid, T. (2013). *Cyber war will not take place.* Oxford University Press, Incorporated.

RISI. (2015). *Online incident database*. https://www.risidata.com

Ritchie, J., Lewis, J., McNaughton Nicholls , C., & Ormston, R. (2014). *Qualitative research practice: A guide for social science students and researchers* (2nd ed.). London.

Robinson, B. (2017, February). *Key facts & data.* Universities Australia. https://www.universitiesaustralia.edu.au/ArticleDocuments/169/Data%20snapshot%202018%20web.pdf.aspx

Rogers, R. W. (1983). *Cognitive and physicological processes in fear appeals and attitude change: A revised theory of protection motivation.* In J. Petty & R. Petty (Eds.), Basic psychopathological research (pp. 153-176)Guilford Press.

Rokeach, M. (1973). *The nature of human values.* Free Press.

Rousseau, D. M. (1996). Changing the deal while keeping the people. *Academy of Management Executives, 10*(1), 50-58. https://doi.org/10.5465/AME.1996.9603293198

Sadler, P. M., Sonnert, G., Hazari, Z., & Tai, R. (2012). Stability and volatility of STEM career interest in high school: A gender study. *Science Education , 96*(3), 411-427. https://doi.org/10.1002/sce.21007

Salopek, D., Zec, M., Mikuc, M., & Vasic, V. (2022). Surgical DDoS filtering with fast LPM. *IEEE Access, 10*, 4200-4208. https://doi.org/10.1109/ACCESS.2022.3140522

Sample, C. (2013). *Culture and computer network attack behavior.* Figshare. http://files.figshare.com/1234667/csample_dissertation_final.pdf

Sample, C., & Karamanian, A. A. (2014). *Hofstede's cultural markers in computer network attack behaviours.* 9th International Conference on Cyber Warfare

and Security 2014, ICCWS. https://www.researchgate.net/publication/288966821_Hofstede's_cultural_markers_in_computer_network_attack_behaviours

Sayfayn, N., & Madnick, S. (2017). *Cybersafety analysis of the Maroochy Shire sewage spill.* Massachusetts Institute of Technology. https://web.mit.edu/smadnick/www/wp/2017-09.pdf

Schjolberg, S., & Ghernaouti-Helie, S. (2011). *A global treaty on cybersecurity and cybercrime* (2nd ed.). Stein Schjølberg and Solange Ghernaouti-Hélie http://pircenter.org/media/content/files/9/13480907190.pdf

Schmidt, N. (2016). *The birth of cyber as a national security agenda.* Department of International Relations, Institute of Political Studies, Faculty of Social Sciences, Charles University.

Schneider, F. B., Sedenberg, E. M., & Mulligan, D. K. (2016). *Public cybersecurity and rationalizing information sharing.* Cornell Bowers Computer Science. https://www.cs.cornell.edu/fbs/publications/publicCybersecRisks.pdf

Schneier, B. (2009, July 13). *So-called cyberattack was overblown.* Schneier on Security. https://www.schneier.com/essays/archives/2009/07/so-called_cyberattac.html

Schulte, S. R. (2008). The WarGames scenario": Regulating teenagers and teenaged technology (1980–1984). *Television & New Media*, *9*(6), 487-513.

Schwalbe, K. (2014). *Information technology project management.* Cengage Learning.

Schwartz, S. H. (2012). An overview of the Schwartz theory of basic. *Online Readings in Psychology and Culture*, *2*(1). https://scholarworks.gvsu.edu/cgi/viewcontent.cgi?article=1116&context=orpc

Shadman, R. (2017, February 2). *Default passwords for most IP network camera brands*. Custom Video Security. https://customvideosecurity.com/research/blog/default-passwords-for-most-ip-network-camera-brands/

Shah, M. A., Elyas, T., & Nasseef, O. (2013). Research paradigms: A slippery slope for fresh researchers. *Life Science Journal, 10*(4).

Shah, S. (2012). *Counting the cost of a DDoS attack. Computing, , 8* http://search.proquest.com.ezproxy.une.edu.au/trade-journals/counting-cost-ddos-attack/docview/1020617766/se-2

Shah, S. (2019, January 3). *7 Biases to avoid in qualitative research*. Editage Insights. https://www.editage.com/insights/7-biases-to-avoid-in-qualitative-research

Shanahan, D. (2015, May 13). *Why perpetuate a 300-year-old anachronism? Reincarnating the research article into a 'living document'* [Blog]. London School of Economics and Political Science. https://blogs.lse.ac.uk/impactofsocialsciences/2015/05/13/reincarnating-the-research-article-into-a-living-document/

Shapira, R. (2019). Leaders' timely succession: Neither term limits nor "golden parachutes," rather periodic tests of trust ascendance. *Journal of Applied Social Science, 13*(2), 180-196. https://doi.org/10.1177/1936724419876301

Sharwood, S. (2021, June 16). *Alibaba suffers billion-item data leak of usernames and mobile numbers*. The Register. https://www.theregister.com/2021/06/16/alibaba_tabao_scraped_data_leak/

Shatskaya, E., Samarina, M., & Nekhorosheva, K. (2016). *PESTEL analysis as a tool of strategic analysis.* Science and Practice: a New Level of Integration in the Modern World - 2nd International Conference. B&M Publishing.

Sherry, J. (2015, August 18). *A ten minute introduction to middleboxes.* Stanford University: http://yuba.stanford.edu/~huangty/sigcomm15_preview/mbpreview.pdf

Shimamoto, D. (2012, March 1). A strategic approach to IT budgeting. *Journal of Accountancy*. https://www.journalofaccountancy.com/issues/2012/mar/20114439.html

Shultz, S. M., & Badan, C. L. (2009). Are we there yet? When is a literature review complete? *American Journal of Nursing, 109*(9), 78-79.

Simon, D. M. (2011). *Assumptions, limitations and delimitations. Dissertation and scholarly research: Recipes for success.* Dissertation Success.

Simon, S. J. (2004). *Rigor vs. delevance: Why can't we all just get along?* Inzicht & Impact. https://www.inzichtimpact.nl/uploads/8/3/4/7/83474572/rigor_vs_relevance_s.j._simon.pdf

Skatsson, J. (2020, August 6). *Cyber security plan will centralise government networks.* Government News. https://www.governmentnews.com.au/cyber-security-plan-will-centralise-govt-networks/

Skilijic, A. (2020, October 12). Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats. *International Cybersecurity Law Review, 1*, 51-61. https://doi.org/10.1365/s43439-020-00014-3

Slavin, R. E. (1984). *Research methods in education: A practical guide.* Prentice-Hall.

Small Enterprise Association of Australia and New Zealand. (2022). *About us.* https://seaanz.org/about-us/

Smith, D. (2017, September 28). *The growth of DDoS-as-a-Service: Stresser services.* Medium. https://medium.com/@RadwareBlog/the-growth-of-ddos-as-a-service-stresser-services-2b93bef1a725

Smith, S. (2014, Nov 19). *5 Famous botnets that held the internet hostage* [Video]. YouTube. https://www.youtube.com/watch?v=A4u_WDCr5h0&feature=youtu.be

Snowdon, M. A. (2015). *The perception of cyber threats and its associative relationship to the protection motivation theory and generational age groups: A quantitative study* [PhD thesis, Capella University]. ProQuest Dissertations Publishing, 3682585.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333-339.

Somani, G., Gaur, M., Sanghi, D., & Conti, M. (2016, Nov 9). DDoS attacks in cloud computing: Collateral damage to non-targets. *Computer Networks, 109*(2), 157-171. https://doi.org/10.1016/j.comnet.2016.03.022

Song, H., Srinivasan, R., Sookoor, T., & Jeschke, S. (2017). *Smart cities : foundations, principles, and applications.* John Wiley & Sons.

Shah, S. (2012). *Counting the cost of a DDoS attack. Computing, , 8* http://search.proquest.com.ezproxy.une.edu.au/trade-journals/counting-cost-ddos-attack/docview/1020617766/se-2

Spadafora, A. (2020, July 18). *AWS hit by major DDoS attack.* Tech Radar. https://www.techradar.com/au/news/aws-hit-by-major-ddos-attack

Standards Australia. (2021, November 9). *Explore catalogue.* https://store.standards.org.au/explore-catalogue

Stoll, C. (1989). *The cuckoo's egg.* Double Day.

Sucuri. (2019, August 9). *What is a DDoS attack?* https://sucuri.net/guides/what-is-a-ddos-attack/

Sundar, V. (2017, March 28). *12 most notorious hacks history*. Indusface. https://www.indusface.com/blog/12-notorious-hacks-history/

Swami, R., Mayank, D., & Virender, R. (2020). Software-defined networking-based DDoS defense mechanisms. *ACM Computing Surveys, 52*(2), 1-36. https://doi.org/10.1145/3301614

Swift, J. (2017, October 12). *GitHub's latest state of the octoverse* . I Programmer. https://www.i-programmer.info/news/136-open-source/11210-github-state-.html

Tanner, J., & Raymond, M. (2012). *Marketing principles version 2.0*. Mountain View: Creative Commons.

Technology Org. (2018, Dec 6). *A guide to HTTP floods: What they are, and what it means to get hit with one*. Technology Org. https://www.technology.org/2018/12/06/a-guide-to-http-floods-what-they-are-and-what-it-means-to-get-hit-with-one/

TeleGeography. (2020, November 26). *Submarine cable map*. Submarine Cable Map, https://www.submarinecablemap.com/

Telstra. (2017, November 26). *Demand for data growing throughout state*. The Examiner. https://www.examiner.com.au/story/5079626/demand-for-data-growing-throughout-state/

Telstra. (2022). *Internet plans*. https://www.telstra.com.au/internet/plans

The White House. (1984, September 17). *National policy on telecommunications and automated information systems security*. Federation of American Scientists. https://fas.org/irp/offdocs/nsdd145.htm

Thody, A. (2011). *Writing and presenting research* (SAGE Study Skills Series).SAGE Publications Ltd.

Thomas, K. (2015, July 16). *British teenager sentenced for massive Spamhaus attack*. We Live Security. https://www.welivesecurity.com/2015/07/16/british-teenager-sentenced-massive-spamhaus-attack/

Thompson, K. (2015, May 18). *Positivism and interpretivism in social research*. ReviseSociology. https://revisesociology.com/2015/05/18/positivism-interpretivism-sociology/

Thompson, W. R., & Dreyer, D. R. (2012). *Handbook of international rivalries, 1494-2010.* CQ Press.

Tidy, J. (2020, September 18). *Police launch homicide inquiry after German hospital hack.* BBC. https://www.bbc.com/news/technology-54204356

Times Higher Education. (2018, October 1). *Best universities in Australia 2019*. https://www.timeshighereducation.com/student/best-universities/best-universities-australia#survey-answer

Torres, N., Pinto, P., & Lopes, S. I. (2021). Security vulnerabilities in LPWANs–An attack vector. *Applied Sciences, 11*(7), 3176. https://doi.org/10.3390/app11073176

Tremlett, G. (2013, May 20). *The man who 'nearly broke the internet'*. The Guardian. https://www.theguardian.com/technology/2013/may/20/man-accused-breaking-the-internet

Trend Micro. (2021). *Attacks from all angles: 2021 midyear cyber security report*. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup

Treasury Portfolio Ministers. (2015, March 17). *Two men sentenced in Australia's largest insider trading case*. The Treasury. https://ministers.treasury.gov.au/ministers/josh-frydenberg-2014/media-releases/two-men-sentenced-australias-largest-insider-trading

Tung, L. (2022, March 2). *DDoS attackers have found this new trick to knock over websites*. ZDNet. https://www.zdnet.com/article/attackers-now-hit-firewalls-to-knock-out-websites/

Turner, C. (2021). Grounded theory: What makes a grounded theory study? *European Journal of Cardiovascular Nursing, 20*(3), 285-289. https://doi.org/10.1093/eurjcn/zvaa034

Turton, W., & Mehrotra, K. (2021, June 5). *Hackers breached colonial pipeline using compromised password*. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

UCL. (2016, March 15). *The main reasons why ethical approval is required*. UCL. https://ethics.grad.ucl.ac.uk/why-is-ethical-approval-required.php

University of New England. (2017a, January 12). *Human research ethics*. http://www.une.edu.au/research/ethics-and-grants/human-research-ethics

University of New England. (2017b). *Management and storage of research data and materials policy*. http://policies.une.edu.au/view.current.php?id=00208

University of New England. (2019a, March 3). *Data storage and backup.* https://www.une.edu.au/staff-current/staff-services/it-services/server-space

University of New England. (2019b, June 12). *Researcher resources*. https://www.une.edu.au/research/ethics-and-grants/human-research-ethics/hrec-forms

University of New England. (2020). *Ethics and grants*. https://www.une.edu.au/research/ethics-and-grants

University of New England. (2022a). *Three minute thesis*. Retrieved from UNE: https://www.une.edu.au/research/hdr/three-minute-thesis

University of New England. (2022b). *UNE Postgraduate Conference 2022.* https://www.une.edu.au/research/hdr/postgraduate-conference

United Nations. (2018). *Australia*. https://sustainabledevelopment.un.org/memberstates/australia#:~:text=Australia%20is%20committed%20to%20the,of%20people%20across%20the%20world.

United Nations. (2022a). *The 17 goals*. https://sdgs.un.org/goals

United Nations. (2022b), *Role of Science, Technology and Innovation for achieving sustainable development.* https://en.unesco.org/events/role-science-technology-and-innovation-achieving-sustainable-development

University of Melbourne. (2018a, January 18). *Do I need ethics approval?* https://staff.unimelb.edu.au/research/ethics-integrity/human-ethics/faq/do-i-need-ethics-approval

University of Melbourne. (2018b, May). *Risk assessment methodology.* http://safety.unimelb.edu.au/__data/assets/pdf_file/0007/1716712/health-and-safety-risk-assessment-methodology.pdf

University of New South Wales. (2019, December 4). *Getting started on your literature review*. https://student.unsw.edu.au/getting-started-your-literature-review

Valeriano, B., & Ryan, M. (2014). The dynamics of cyber conflict between rival antagonists, 2001-2011. *Journal of Peace Research, 51*(3), 347-36.

Varghese, S. (2019, June 18). *Linux devices vulnerable to ping of death attack*. IT Wire. https://itwire.com/security/linux-devices-vulnerable-to-ping-of-death-attack.html

Verizon. (2021, August 26). *Small business data breaches: The latest findings*. https://www.verizon.com/business/small-business-essentials/resources/small-business-data-breaches-the-latest-findings/

Vijayan, J. (2020, August 5). *DDoS attacks doubled in Q2 compared with prior quarter*. Dark Reading. https://www.darkreading.com/attacks-breaches/ddos-attacks-doubled-in-q2-compared-with-prior-quarter

Vishwakarma, R., & Jain, A. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication Systems, 73*(1), 3-25.

Vishwakarma, R., & Jain, A. K. (2019). A survey of DDoS attacking techniques and defence mechanisms. *Telecommunication Systems, 1*(23). https://doi.org/10.1007/s11235-019-00599-z

Vlajic, N., & Zhou, D. (2018, July). IoT as a land of opportunity for DDoS hackers. *Computer, 51*(7), 26-34. https://doi.org/10.1109/MC.2018.3011046

Vocus. (2018, June 5). *Best practice to reduce the risk of toll fraud.* https://www.vocus.com.au/news/best-practice-to-reduce-the-risk-of-toll-fraud

Wagner, T., Palomar, E., Mahbub, K., & Abdallah, A. E. (2018). A novel trust taxonomy for shared cyber threat intelligence. *Security and Communication Networks, 2018*. https://doi.org/10.1155/2018/9634507

Walkowski, D. (2019, June 5). *What is a DDoS attack?* F5. https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-

Walter, C. (2005). Kryder's law. *Scientific American, 293*(2), 32-33.

Walters, K. A., & Hamrell, M. R. (2008). Consent forms, lower reading levels, and using flesch–kincaid readability software. *Drug Information Journal, 42*(4), 385-394.

Wang, J. I. (2016, December 12). *Largest DDoS attack each year*. The Atlas. https://www.theatlas.com/charts/rJ3Y0ynmg

Wang, Z. H., & Sun, L. (2021). Effect mechanisms, human vulnerabilities and attack methods. *Social Engineering in Cybersecurity, 9,* 11895-11910. https://doi.org/10.1109/ACCESS.2021.3051633

Warburton, D. (2021, May 7). *DDoS attack trends for 2020*. F5. https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020

Ward, M. (2015, February 6). *Why small firms struggle with cyber security*. BBC. https://www.bbc.com/news/technology-31039137

Weagle, S. (2016, October 7). *The IoT Makes it easier to launch massive DDoS attacks*. Coreo. https://www.corero.com/blog/764-the-iot-makes-it-easier-to-launch-massive-ddos-attacks.html

Webber Insurance Services. (2022). *The complete list of data breaches for 2018-2022*. https://www.webberinsurance.com.au/data-breaches-list#twentytwo

Westbrook, T., & Blanchard, B. (2018, July 6). *Top-ranked Australian university hit by Chinese hackers: media*. Reuters. https://www.reuters.com/article/us-australia-cyber/top-ranked-australian-university-hit-by-chinese-hackers-media-idUSKBN1JW1KE

Westland, J. (2018, March 22). *The triple constraint in project management: Time, scope & cost*. Project Manager. https://www.projectmanager.com/blog/triple-constraint-project-management-time-scope-cost

Whitman, M. E., & Mattord, H. J. (2017). *Management of information security* (5th ed.). . Cengage.

Whitten-Woodring, J. (2009). Watchdog of lapdop? Media treedom, regime type, and government respect for human rights. *International Studies Quarterly, 53,* 595-625.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking, 17*(3), 131-132.

Wigmore, I. (2019, December). *Ghosting (in the workplace)*. What Is. https://whatis.techtarget.com/definition/ghosting#:~:text=Ghosting%20is%20to%20cease%20communications,potential%20employees%20who%20suddenly%20disappear.

Wildavsky, A., & Dake, K. (1990). Theories of risk perception: Who fears what and why? *Daedalus, 119*(4), 41-60.

Williams, O. (2019, March 11). *Businesses are failing to adequately report data breaches*. New Statesman Tech. https://tech.newstatesman.com/security/data-breach-reports-ico

Willig, C. (2013). *Introducing qualitative research in psychology* (3rd ed.). McGraw-Hill Education.

Wirth, A. (2020). Cyberinsights: COVID-19 and what it means for cybersecurity. *Biomedical Instrument Technology, 54*(3), 216-219. https://doi.org/10.2345/0899-8205-54.3.216

Wolff, J. (2019, January 16). *Practice hacktivism at your own risk*. Slate. https://slate.com/technology/2019/01/martin-gottesfeld-hacktivism-ddos-boston-childrens-justina-pelletier.html

Woolf, N. (2016, October 27). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Wu, J., & Lam, O. (2017, September 3). *The evolution of China's Great Firewall: 21 years of censorship*. Hong Kong Free Press. https://www.hongkongfp.com/2017/09/03/evolution-chinas-great-firewall-21-years-censorship/

Wu, W., Shi, K., Wu, C.-H., & Liu, J. (2022). Research on the impact of information security certification and concealment on financial performance: Impact of ISO 27001 and concealment on performance. *Journal of Global Information Management, 30*(3), 1-16. https://doi.org/10.4018/jgim.20220701.oa2

Wueest, C. (2014, October 21). *The continued rise of DDoS attacks*. Symantec. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/continued-rise-of-DDoS-attacks-14-en.pdf

Xiaoming, H., & Chow Seet K. (2004). Factors affecting internet development: An Asian survey. *First Monday, 9*(2), 1-22.

Xie, B., Charness, N., Fingerman, K., Kaye, J., Khurshid, A., & Kim, M. T. (2020). When going digital becomes a necessity: Ensuring older adults' needs for information, services, and social inclusion during COVID-19. *Journal of Aging & Social Policy, 32*(4-5), 460-470. https://doi.org/10.1080/08959420.2020.1771237

Yoachimik, O., & Ganti, V. (2022, January 10). *DDoS attack trends for Q4 2021*. Cloudflare. https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/

York, K. (2016, October 22). *Read Dyn's statement on the 10/21/2016 DNS DDoS attack*[Blog]. DYN. https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

Yuan, J., & Mills, K. (2005). Monitoring the macroscopic effect of DDoS flooding attacks. *IEEE Transactions on Dependable and Secure Computing, 2*(4), 324-335. https://doi.org10.1109/TDSC.2005.50

Zetter, K. (2016, March 3). *Inside-cunning-unprecedented-hack-ukraines-power-grid*. Wired. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zhou, W., Jia, W., Wen, S., Xiang, Y., & Zhou, W. (2014). Detection and defense of application-layer DDoS attacks in backbone web traffic. *Future Generation Computer Systems, 38*(36).

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2010). *Business research methods* (8th ed.). South-Western Cengage Learning.

Appendices

Appendix A – Participant Information Sheet

UNE Business School
University of New England
Armidale NSW 2351
Australia
Phone +6[redacted]
iwiltshi@myune.edu.au

INFORMATION SHEET
for
PARTICIPANTS

I wish to invite you to participate in my research project, described below.

My name is Ian Wiltshire and I am conducting this research as part of my PhD in the School of Business at the University of New England. My supervisors are Dr Sujana Adapa and Dr David Paul.

Research Project	**Distributed Denial of Service (DDoS) Attacks – Development of a Readiness Tool**
Aim of the Research	The aim of this research is to gain understanding of the current knowledge, focus and capability (related to DDoS threats) within the Australian Business community. This study intends to interview IT staff in Australian businesses who have had, or are likely to have direct interaction with DDoS events to explore personal, team and organisational perceptions of DDoS risks and consequences within the Australian University context.
Interview	I would like to conduct a face-to-face interview with you, which can occur via videoconference, at your workplace or at a nearby café of your choice. I estimate that the interview will take approximately one hour. With your permission, I will make an audio recording of the interview to ensure that I accurately recall the information you provide and for later transcription. Following the interview, if you wish to receive a copy of the transcription, one can be provided.
Confidentiality	Any personal details gathered in the course of the study will remain confidential. No individual or organisations will be identified by name in any publication of the results. All names will be replaced by pseudonyms; this will ensure your anonymity. If you agree I would like to quote some of your responses. This will also be done in a way to ensure that you are not identifiable.
Participation is Voluntary	Please understand that your involvement in this study is voluntary and I respect your right to stop participating in the study at any time without consequence and without needing to provide an explanation.
Questions	The interview questions will not be of a sensitive nature: rather they are general, and will enable us to enhance our knowledge of individual, team and organisational knowledge, focus and capability with regard to DDoS attacks.
Use of Information	I will use the information gathered from the interview as part of my research, which is expected to complete in 2021. Information gathered from the interview will be used in academic journal articles and conference presentations both before and after this date. At all times, your identity will be protected by presenting the information using methods that prevent identification.

Upsetting Issues	It is unlikely that this research will raise any personal or upsetting issues but if it does you may wish to contact your local Community Health Centre or Lifeline on 13 11 14.
Storage of Information	I will keep all hardcopy notes and recordings of the interviews in a locked cabinet in my place of residence at the time of data collection. Any electronic data will be kept on cloud.une.edu.au (UNE's centrally managed cloud server managed by the research team). It will also be kept on a password protected computer and mobile phones in the same locations. Only the research team will have access to the data.
Disposal of Information	All the data collected in this research will be kept for a minimum of five years after successful submission of my portfolio, after which it will be disposed of by deleting relevant computer files and destroying or shredding hardcopy materials.
Approval	This project has been approved by the Human Research Ethics Committee of the University of New England (Approval No. HE18-205, Valid to 30/03/2021).
Researchers Contact Details	Feel free to contact me with any questions about this research by email at iwiltshi@myune.edu.au or by phone on +61 [redacted] You may also contact my supervisors'. My Principal supervisor's name is Dr Suiana Adapa and she can be contacted by email at sadapa2@une.edu.au or by phone on 02 6773 2915 and my Co-supervisor's name is Dr David Paul and his email address is dpaul4@une.edu.au and phone number is 02 6773 2447.
Complaints	Should you have any complaints concerning the manner in which this research is conducted, please contact: Mrs Jo-Ann Sozou Research Ethics Officer Research Services University of New England Armidale, NSW 2351 Tel: (02) 6773 3449 Email: ethics@une.edu.au
	Thank you for considering this request and I look forward to further contact with you. Regards, Ian Wiltshire

Appendix B – Participant Consent Form

CONSENT FORM
for PARTICIPANTS

Research Project: Distributed Denial of Service (DDoS) Attacks:
Development of a Readiness Tool

I, ……., have read the information contained in the Information Sheet for Participants and any questions I have asked have been answered to my satisfaction.	Yes/No
I agree to participate in this activity, realising that I may withdraw at any time.	Yes/No
I agree that research data gathered for the study may be quoted and published using a pseudonym.	Yes/No
I agree to having my interview audio recorded and transcribed.	Yes/No
I would like to receive a copy of the transcription of the interview.	Yes/No
I am older than18 years of age.	Yes/No

…… ……
Participant Date

Appendix C – Interview Questions

Interview Questionnaire

Screening questions

1. Have you heard of DDOS attacks?
2. If yes, are you comfortable with answering questions regarding DDOS attacks within your organisation?

If **Yes** – proceed, if **No** - terminate interview.

Section 1 – Individual skills and capabilities

1. What is your level of understanding of DDOS attacks?
2. Do you consider DDOS to be a real threat to your organization?
3. What Cyber Security event would you consider to be a greater risk?
4. Are there any formal contingency plans in place within your organisation to mitigate the DDOS attacks in the future?
5. Can you describe the steps taken to build these plans?
6. What was the motivation for your mitigation plan?

Section 2 – Team skills and capabilities

1. Within the team, who would you say are the most important stakeholders?
2. Is there involvement from other stakeholders (in the process), that you think are less important to those identified above?
3. What are the challenges you might face while implementing a DDOS mitigation plan?
4. Have you made plans to address these challenges?
5. Does the existing team within the organisation have the required skills and capabilities to identify and respond to DDOS attacks?
6. How do you think your team could increase these skills and capabilities?

Section 3 – Organisations plans and motivation for capability

1. Do large organisations that have a specific IT department have some sort of understanding about DDOS
2. Does the organisation you work for have a specific IT department?
3. Do you think the organisation considers the threat of DDOS attack as more, less or the same as your own level of threat assessment?
4. How has the organisations threat perception change over the last few years?
5. How do you think the organisation could enhance the teams' future skills and capabilities to tackle DDOS attacks?
6. Do you think this is the responsibility of the organisation?
7. What do you think is the role of industry?
8. What do you think is the role of government?

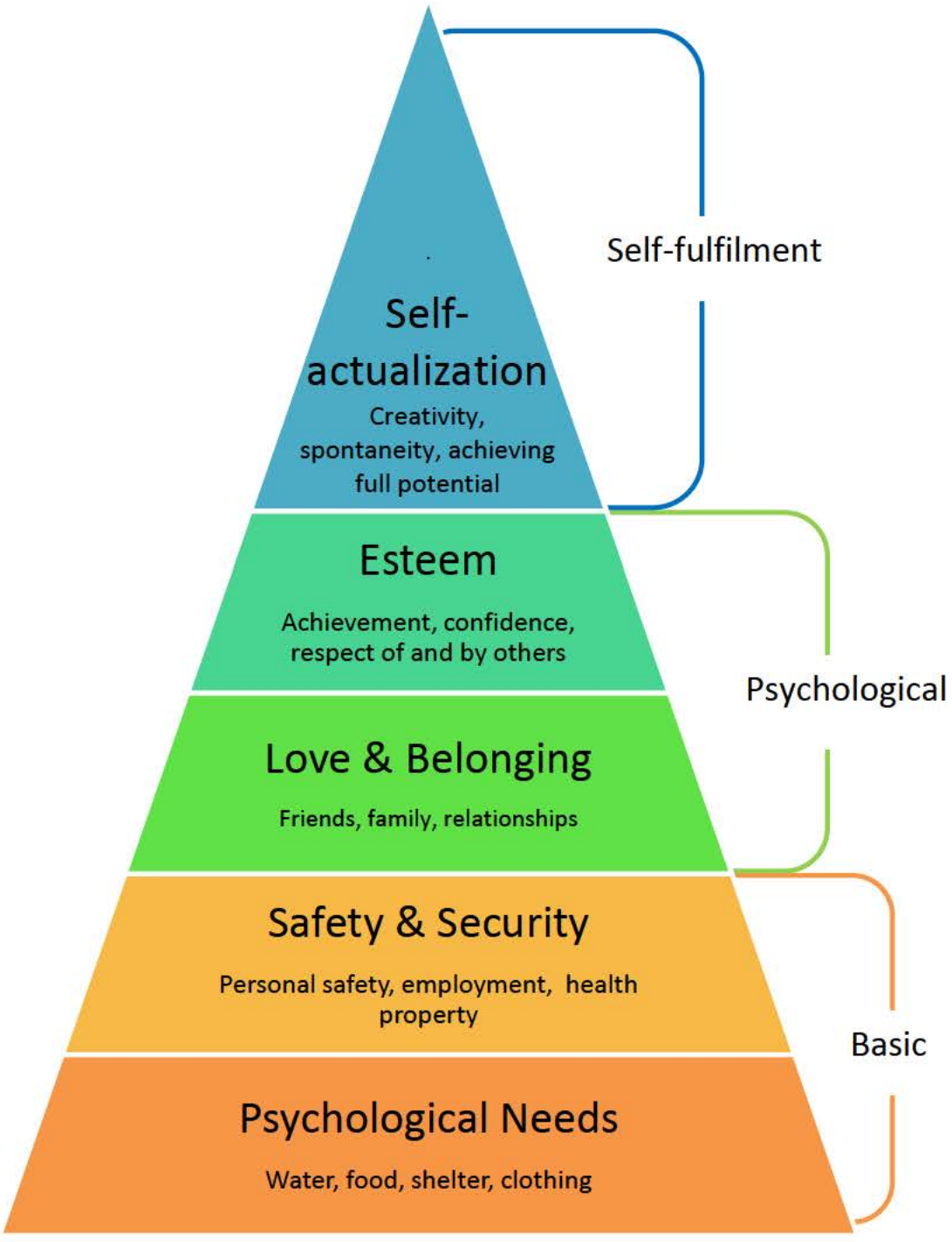
Section 4 - Demographic Questions

1. Describe your role in the organization?
2. How long have you been in this role?
3. How would you describe you level of authority, particularly in regard to decisions which address security and DDOS events?
4. What is the size of your team?
5. What scale of resources are allocated to the DDOS problem?

Thank you!

Appendix D – Referenced Theories

Maslow's Hierarchy of Needs (adapted from Tanner & Raymond (2013))



McClelland's trio of needs (adapted from McClelland (2010))

Appendix E – Website Analysis Questions

Company ID - (O1-O60)
Reason Refused – (If employee in organisation was invited to participate in interview)
Company Size (M/L)
What is the detail type? e.g., Generic/Detailed
Is there a process available to report a security incident?
Are there any security related downloads?
Is security training offered?
Count of paragraphs related to cyber security?
Count of sentences related to cyber security?
How many images are used?
Any comments on the visual aesthetic.
Is there a Live Feed?
Is there a Chat Box?
Is there a contact list? (What does it show, individuals or Generic addresses?)
Are there any relationships with other organisations (related to cyber security)?
Is there a recent incident log or blog?
What industry do they identify with (sector from ABS)?
Has the organisation listed any of their publicly reported data breaches?
Do they have any publicly listed data breaches published on 3rd party websites?
Which Australian states are the organisations located or are they National?
Flesch–Kincaid reading ease score
Flesch–Kincaid grade level
Flesch–Kincaid grade and age

Appendix F – Approached Roles

Role of respondents approached
Associate Director
Business Development Manager
CEO
Chief Data Officer
Chief Information Officer
Chief Information Security Officer
Chief Technology Officer
Cloud Network Engineer
Digital Solutions Lead
Enterprise Platform Engineer
Enterprise Security Architect
General Manager Operations
Group IT Service Delivery Manager
Head of ICT Strategy, Services and Operations
Head of Solution Architecture
ICT Security Manager
Information Security Analyst
IT Helpdesk
IT Manager, Information Security
IT Operations Manager
IT Security Analyst
IT Security Manager
IT Security Specialist
Manager Cyber Security
Manager Information Systems
Manager, Security Services
Product Manager
Program Leader
Senior Information Security Officer
Senior IT Network Security Specialist
Senior Systems Administrator
Site Reliability Engineer
Vice President and General Manager

Appendix G – Participant Demographics

ID	Role	Tenure (Years)	Team Size	Sector (ABS)	Gender	States/ National	Company Size (ABS)
P1	Global Product Manager.	1	240	Information Media and Telecommunications	Male	VIC	Large
P2	Information Security Adviser	2	11	Education and Training	Male	NSW	Large
P3	Partner	3	25	Professional, Scientific and Technical Services	Male	QLD	Medium
P4	Operations Management	1	4	Information Media and Telecommunications	Male	National	Medium
P5	IT Manager, Information Security	3	11	Education and Training	Male	NSW	Large
P6	Systems Administrator	10	6	Retail Trade	Male	National	Large
P7	ICT Operations Manager	16	12	Education and Training	Male	QLD	Large
P8	Manage a team of IT Engineers	2	5	Information Media and Telecommunications	Male	National	Large
P9	Associate Director - Enterprise Architecture, Security and Governance	3	5	Education and Training	Male	NSW	Large
P10	Head of IT Security	3	3	Information Media and Telecommunications	Female	National	Medium

ID	Role	Tenure (Years)	Team Size	Sector (ABS)	Gender	States/ National	Company Size (ABS)
P11	General Manager	2	6	Information Media and Telecommunications	Male	National	Medium
P12	Senior Information Security Officer	5	7	Education and Training	Female	NSW	Large
P13	Manager	2	10	Information Media and Telecommunications	Male	National	Large
P14	System Administrator	14	10	Information Media and Telecommunications	Male	National	Medium
P15	Security Consultant	6	1	Retail Trade	Male	QLD	Medium
P16	Quality Engineer	0.5	15	Retail Trade	Male	QLD	Large
P17	IT security analyst	0.5	9	Education and Training	Male	NSW	Large
P18	Security and Network Engineer	3	8	Professional, Scientific and Technical Services	Male	TAS	Medium
P19	Manager - Information Security Management.	4	6	Education and Training	Female	WA	Large
P20	Team Lead - Helpdesk	8.5	50	Professional, Scientific and Technical Services	Male	National	Large
P21	Manager - Information Management	4	5	Public Administration and Safety	Male	VIC	Medium
P22	Team Leader - Systems Administration	0.5	70	Professional, Scientific and Technical Services	Male	QLD	Large
P23	IT Security Manager	2	5	Healthcare and Social Assistance	Male	QLD	Large

ID	Role	Tenure (Years)	Team Size	Sector (ABS)	Gender	States/ National	Company Size (ABS)
P24	IT Manager	8	14	Professional, Scientific and Technical Services	Male	National	Large
P25	Service – Design and Implementation	10	10	Information Media and Telecommunications	Male	National	Large
P26	Systems Administrator	25	12	Professional, Scientific and Technical Services	Male	National	Large
P27	Senior Systems Specialist	5	8	Professional, Scientific and Technical Services	Male	QLD	Large
P28	Senior Systems Engineer	4	45	Information Media and Telecommunications	Male	National	Large
P29	Head of Technology	4	110	Retail Trade	Female	National	Large
P30	Systems Engineer	5	25	Mining	Male	National	Large

Appendix H – Summary of Theories

Theory framework	Definition	Previous use	In use	Why/Why not
Ontology	The nature of reality			
Realism	Philosophical reality exists independently.	Realism has previously been applied by researchers and practitioners analysing historical events.	Yes	Realism was considered where data that could be independently verified existed. E.g., Demographics data.
Idealism	Philosophical reality exists through belief and understanding.	Researchers have used idealism when seeking to understand the motivations of cyber attackers and how individuals respond to threats.	Yes	Idealism occurred when analysing interview information as the nature of questions sought to understand the perspectives constructed by those interviewed.
Epistemology	The nature of knowledge			
Empirical knowledge	Knowledge gained through a personal understanding of sensory experiences	Cyber security employees used empirical knowledge to develop their cyber security strategies.	Yes	During research interviews and data collection, empirical knowledge was developed as the researcher used sensory experiences to gather and understand.
Intuitive knowledge	Faith, intuition, and instinct are relied upon for understanding.	Intuitive knowledge used to derive new theories when based on empirical and logical understanding.	Yes	As existing knowledge regarding DDoS perception was minimal, intuition and intuitive knowledge were used to develop initial

Theory framework	Definition	Previous use	In use	Why/Why not
				research goals and starting points for exploratory research.
Logical knowledge	Knowledge is derived from the understanding of theoretical concepts	Logical knowledge has been used to theorise outcomes based of known circumstances.	Yes	Logical knowledge allowed sources of authoritative knowledge to be combined, establishing firmer credibility of theories, and building a solid base of subject knowledge.
Authoritative knowledge	Knowledge is received through teaching or reading.	Authoritative knowledge was used by researchers as they learned to understand how critical research is performed. This included using established theories and frameworks such as Kolenko, 2019 research of cultural patterns and behaviour.	Yes	Initially, authoritative learning provided the base of knowledge for both the project proposal and literature review stages. Then throughout the remainder of the project, authoritative knowledge became the base on which new understanding was built.
Methodology	Research design, methods processes and attributes			
Quantitative analysis	Mathematical approach to data analysis.	Quantitative analysis was used to analyse the data collected on cyber-attacks through previous years.	Yes	Quantitative analysis was used to analyse existing numerical data and demographic information.
Qualitative analysis	Subjective analysis of data that cannot	Qualitative analysis was used by researchers to gain understanding and insights into non-numeric data.	Yes	Quantitative analysis was applied to analysis of websites and interviews to understand the meaning behind the data.

Theory framework	Definition	Previous use	In use	Why/Why not
	be analysed numerically.			
Document analysis	Interpretation and understanding of physical and electronic documents.	Document analysis was used in the analysis of existing literature.	Yes	Document analysis was used to understand the meaning behind the depth and quality of published organisational data.
Grounded theory	Development of theories based (grounded in) the actual data collected.	Research, such as Rogers 1983, while initiated by Rogers Protection Motivation Theory (PMT), used actual collected data to formulate a revision of the PMT theory.	Yes	Grounded theory was adopted as exiting theories did not meet the requirements of the study. A lack of existing data drove the need for explorative research from which theories were developed.
Axiology	The value of the research			
Extrinsic value	Knowledge value is realised in the application of the knowledge.	Extrinsic value has been observed in research such as, from A10 Networks, Kaspersky and Radware, as the knowledge gained leads directly to organisational change.	Yes	Most of the value of the knowledge gained by this research was realised in the new understandings that could lead to change and in recommendations provided to individuals, organisations, and Governments.

Theory framework	Definition	Previous use	In use	Why/Why not
Intrinsic value	Knowledge value is realised in the knowledge itself.	Intrinsic value has also been observed in research from A10 Networks, Kaspersky and Radware as these companies maintain reputation and credibility through continued research.	Yes	A level of intrinsic value is obtained by the researcher and readers of this thesis through feelings of achievement and confidence delivered through greater understanding of the topic.
Research Paradigms	Research Framework			
Positivist	Research is studied objectively and passively.	Previous research measured statistics against established standards and previous results.	Yes	A positivist perspective was adopted when analysing quantitative data, collected from independent sources.
Interpretivist	Relationships with the subject are vital to understand meaning.	Interpretive research occurs when the results pass through the researcher as they are collected. Previous research through interview where the meaning is uncovered by the researcher use this framework.	Yes	An interpretivist perspective was adopted when analysing interviews and documents due the inseparable interaction between researcher and the understanding of the data.
Constructivism	Researcher influence cannot be removed from the	Research that involves human experience can be considered somewhat constructive due to the influence of the human mind.	Yes	The researcher played a small part in the construction of the data, as the interview questions followed a guided and predetermined

Theory framework	Definition	Previous use	In use	Why/Why not
	construction of findings.			path which may have mildly influenced responses.
Critical theory	Researcher values or biases, influence the understanding of independently existent data.	Research from Sample, 2013 and Snowdon, 2015 both used critical theory to evaluate existing theories using secondary data with the intent of producing cultural impact.	Yes	Critical theory was undertaken as implications and recommendations were founded.