NELSON MANDELA
UNIVERSITY

CYBERSECURITY:
REDUCING THE ATTACK SURFACE

INAUGURAL LECTURE

by

Professor Kerry-Lynn Thomson

delivered at Nelson Mandela University

on 26 August 2021

Faculty of Engineering, the Built Environment and Technology

Inaugural & Public Lectures

2021

ABSTRACT

Almost 60% of the world’s population has access to the internet and most organisations today rely on internet connectivity to conduct business and carry out daily operations. Further to this, it is estimated that concepts such as the Internet of Things (IoT) will facilitate the connections of over 125 billion ‘things’ by the year 2030. However, as people and devices are becoming more and more interconnected, and more data is being shared, the question that must be asked is – are we doing so securely?

Each year, cybercriminals cost organisations and individuals millions of dollars, using techniques such as phishing, social engineering, malware and denial of service attacks. In particular, together with the Covid-19 pandemic, there has been a so-called ‘cybercrime pandemic’. Threat actors adapted their techniques to target people with Covid-19-themed cyberattacks and phishing campaigns to exploit their stress and anxiety during the pandemic.

Cybersecurity and cybercrime exist in a symbiotic relationship in cyberspace, where, as cybersecurity gets stronger, so the cybercriminals need to become stronger to overcome those defenses. And, as the cybercriminals become stronger, so too must the defenses. Further, this symbiotic relationship plays out on what is called the attack surface.

Attack surfaces are the exposed areas of an organisation that make systems more vulnerable to attacks and, essentially, is all the gaps in an organisation’s security that could be compromised by a threat actor. This attack surface is increased through organisations incorporating things such as IoT technologies, migrating to the cloud and decentralising its workforce, as happened during the pandemic with many people working from home.

It is essential that organisations reduce the digital attack surface, and the vulnerabilities introduced through devices connected to the internet, with technical strategies and solutions. However, the focus of cybersecurity is often on the digital attack surface and technical solutions, with less of a focus on the human aspects of cybersecurity. The human attack surface encompasses all the vulnerabilities introduced through the actions and activities of employees. These employees should be given the necessary cybersecurity awareness, training and education to reduce the human attack surface of organisations. However, it is not only employees of organisations who are online. All individuals who interact online should be cybersecurity aware and know how to reduce their own digital and human attack surfaces, or digital footprints.

This paper emphasises the importance of utilising people as part of the cybersecurity defense through the cultivation of cybersecurity cultures in organisations and a cybersecurity conscious society.

Keywords: cybersecurity, attack surface, cybersecurity culture, cybersecurity awareness

1. Introduction

Almost 60% of the world's population has access to the internet and most organisations today rely on internet connectivity to conduct business and carry out daily operations. Each year, however, cybercriminals cost organisations and individuals millions of dollars, using techniques such as phishing, social engineering, malware and denial of service attacks.

It is essential, therefore, that organisations and individuals reduce both the digital and human attack surfaces, which are frequently exploited by cybercriminals. While the focus of cybersecurity is often on the digital attack surface, the human aspects of cybersecurity must be given equal attention. This paper emphasises the importance of utilising people as part of the cybersecurity defense through the cultivation of cybersecurity cultures in organisations and a cybersecurity conscious society.

2. Increasing Global Digital Connectivity

The world is becoming increasingly connected, as year-on-year more users get access to the internet. There are currently 7.83 billion people on the planet. 4.66 billion people, or 59.5% of the world's population, have access to the internet. Of those, 4.2 billion are active social media users, and 5.22 billion people have access to a mobile device (Hootsuite 2021).

Northern European countries have the highest internet penetration, with an average of 96% of the population accessing the internet. Countries in Eastern Africa have the lowest internet penetration, with an average of 24% of the population accessing the internet. In comparison, 62% of people in Southern Africa have access to the internet (Hootsuite 2021).

South Africa has a population of 59.67 million people and 38.19 million, or 64%, of the population has access to the internet. There are 100.6 million mobile connections in South Africa, which exceeds the population at 168.5%, one of the highest percentages in the world. Further to this, 25 million South Africans are active social media users, with WhatsApp, YouTube, Facebook and Instagram being the most popular social media platforms in South Africa (Hootsuite 2021).

South Africans, aged 16 years to 64 years, spend an average of 10 hours and 6 minutes online per day, which is 3 hours and 10 minutes more than the global average. Activities include streaming television, reading press media, listening to music streaming services and online gaming. South Africans also spend an average of 3 hours and 30 minutes on social media platforms per day. 61% of social media users indicate that they use social media for business purposes, using platforms like LinkedIn, for networking and to engage with entrepreneurs (Hootsuite 2021).

With regard to what is real and what is fake on the internet, 71.6% of South Africans expressed concern about not being able to recognise the difference, compared to 56.4% of people globally. In the age of misinformation, disinformation and fake news, this *should* be a big concern. And 33.1% of people globally expressed a concern over how companies make use of their personal data, compared to 44.5% of South Africans (Hootsuite 2021).

3. The Internet of Things (IoT) and Artificial Intelligence

These statistics highlight that an increasing number of people are getting access to the benefits of the internet and spending more time engaging in online activities and, as a result, the world is becoming more interconnected.

Further to this, the Internet of Things (IoT) is facilitating the connectivity of billions of devices on the internet. One of the definitions of the IoT is the “group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to the data they generate” (Dorsemaine 2015). The IoT devices communicate with the network independently of human action, and use sensors and software to collect and share data. Besides computers, examples of devices that may connect using the IoT include vehicles, smart phones, home appliances, medical instruments and industrial systems, which are all connected and sharing data (Patel & Patel 2016).

According to Statista (2021), there are currently about 21.5 billion devices connected to the internet and its expected that this number will jump to around 125 billion things by 2030 (Martech Advisor 2019). However, these estimates are changing all the time, as newer technologies such as 5G become more mainstream.

Some of the better known IoT implementations are smart homes. Smart homes allow for the integration of technologies and various services using the home network, which should result in a better quality of living. Many aspects of homes, such as lighting, alarm systems, coffee machines, TVs and air conditioners all ‘talk’ to each other to maintain a conveniently automated home – all controlled by a smartphone (Robles & Kim 2010).

However, the IoT is about more than convenience and is set to disrupt many industries. This includes healthcare where it is referred to as the Internet of Medical Things, or IoMT, and includes wearables to monitor heart rate and body temperature, while in future internal sensors may be used for patients where accurate, up-to-the minute and continuously updated data is required (Joyia, et al 2017). In aviation, older engines have approximately 250 sensors to monitor performance and mechanical operations, while modern engines can have up to 5,000 sensors generating up to 10GB of data per second (Aeris 2021).

Much of the data that is collected through the IoT is sent to the cloud for storage. Cloud computing is essentially remote servers hosted on the internet used to store, manage and process data - instead of storing that data on local servers (De Silva 2017). However, as more and more things are connected, more and more data will be generated. It is estimated that, by 2025, the IoT data volume will be around 80 zettabytes (Statista 2021).

Together with increasing data, there are increasing concerns with regard to using the cloud for the volumes of data generated. Downtime issues, security concerns, increased data latency and bandwidth issues are becoming apparent in the cloud computing architectures. To address these issues, fog computing, or edge computing, allows for fog nodes to be placed between the data sources and the cloud. The majority of the data generated is sent to these fog nodes, where computations needing less computing and less storage, can take place. However, cloud services can still be used to manage and analyse large volumes of data (De Silva 2017).

Therefore, there is no need to transmit every bit of data to the cloud for processing, as fog nodes are able to process that data in a more efficiently and provide responses quicker than cloud – which is important for situations where real-time analysis is needed, for instance in the healthcare environment (De Silva 2017).

However, while IoT sensors and devices are capturing huge amounts of data from multiple sources, the processing and analysing of this data remains complex. Therefore, while IoT encompasses all the devices interacting using the internet, it is Artificial Intelligence, or AI, that allows devices to learn from that data and experiences. It is through the convergence of IoT and AI that leads to smart behaviour and decision making with little to no human interference. This AI enabled IoT, or the Artificial Intelligence of Things (AIoT) allows for optimal decisions and discoveries in a fraction of the time that it would take people (Forbes 2019).

Artificial intelligence allows for things like quicker and more accurate diagnosis of diseases; autonomous, self-driving cars and trucks, and virtual tutors to assist lecturers or teachers by using facial analysis to determine students' emotions while in class to see who is struggling or disengaged (Calo et al 2017).

All of these things working together, smart healthcare, smart transportation, smart education, smart traffic, smart energy, smart retail – all these sectors contribute to smart cities. For example, sensors for the early detection of water leaks, smart parking which allows you to check parking availability in the city, smart lighting according to the weather conditions and smart roads that could send warning messages and divert traffic in the event of an accident or traffic jams.

Therefore, the convergence of AI and IoT, together with future advancements in technology, hold many benefits for users and will have far-reaching impacts on how users interact with the world.

However, as the world is becoming more interconnected, and more data is being shared, the question that must be asked is – are we doing so securely? Is security a priority in our increasingly interconnected world?

4. Cyberattacks and Cyberthreats

There are a variety of cyberattacks and cyberthreats and, as more systems are connected to the internet, cyberattacks like ransomware, which originated in cyberspace, are crossing over into the real world.

Ransomware is extortion software that compromises and locks your computer and then demand a ransom to unlock it – or the threat actors may threaten to make private information public if a ransom is not paid (Pascariu & Barbu 2015).

Further, cybercrime has become a booming business. On the Dark Web, there are so-called business models referred to as "cybercrime-as-a-service" where organised criminal groups sell or rent their hacking software or services to those who want to carry out cyberattacks to extort victims (Palmer 2021).

Ransomware no longer only affects online services. In 2017, the WannaCry ransomware attack compromised more than 300, 000 machines in 150 countries. This included 80 hospitals in the UK, who were forced to divert patients after malware prevented medical records from being accessed and where crucial equipment such as MRI scanners and X-ray machines had to be taken offline, while legacy devices and servers in the networks were patched (Landi 2019).

In May 2021, Colonial Pipeline, which accounts for 45% of the US East Coast's fuel supply, was forced to shut down its operations and freeze many of its IT systems after it was hit by a ransomware attack by a group called DarkSide. This led to a shortage in fuel supply along the East Coast for the military, for aviation and for consumers – which led to panic buying in some areas.

These are just two examples of how cyberattacks and cyberthreats can have very real-world impacts. Further, as computers are put in charge of more of the real world, this problem is likely to get worse.

5. Cybercrime Pandemic

Together with the Covid-19 pandemic, there has been a surge in cybercrime – dubbed by some as the ‘Cybercrime Pandemic’ (Fontanilla 2020).

McAfee (2021) observed an average of 648 malware threats per minute in the fourth quarter of 2020. RiskBased Security (2020) indicated that the total number of compromised records was over 37 billion in 2020, an increase of 141% compared to 2019. In addition, there were over 10 million Distributed Denial of Service attacks – up over 20% compared to 2019 – which included DDoS extortion campaigns, where key services were blocked until a ransom was paid. Further, the costliest data breaches were found in the following five industries; Healthcare, Financial, Pharmaceuticals, Technology and Energy (Hummel & Hildebrand 2021; IBM Security 2021).

Cybercrime has cost organisations and individuals millions of dollars during the Covid-19 pandemic alone. According to the Cost of a Data Breach Report 2021, the average cost of a data breach rose from $3.86 million in 2020 to $4.24 million dollars in 2021 – with Customer Personally Identifiable Information (PII) being the costliest type of record lost or stolen in breaches at an average of $180 per record. The average total cost of a ransomware breach as an initial attack vector was $4.62 million, but it was phishing attacks that remained one of the top initial attack vectors (IBM Security 2021).

Phishing attacks are when threat actors try to get sensitive information from a victim by disguising themselves as a trustworthy source. This is most commonly done through phishing emails. It will look like the email is coming from a bank, for example, and there is usually a sense of urgency to the emails, threatening the suspension of an email or bank account, unless a certain action is taken. These phishing emails usually require people to click on links or to send personal information, like usernames and passwords or credit card details. Besides emails, voice notes or voicemails, called vhishing attacks, or sms's, called smishing attacks could be used to try to trick users into giving away information (Lastdrager 2014; Fruhlinger 2020).

Phishing attacks had an average total cost of $4.65 million and a surge of phishing attacks was seen in March and April last year which coincided with stay-at-home orders for people around the world, together with the huge amount of misinformation and disinformation about Covid-19 that started doing the rounds. Threat actors adapted their techniques to target people with Covid-19-themed phishing campaigns to exploit the stress and anxiety during the pandemic (IBM Security 2021).

There is a constant tension in cyberspace between cybersecurity and cybercrime. They exist in a symbiotic relationship, where, as cybersecurity gets stronger, so the cybercriminals need to get stronger to overcome those defenses. And, as the cybercriminals get stronger, so too must the defenses. Further, this symbiotic relationship plays out on what is called the attack surface.

6. Attack Surfaces

According to NIST, the definition of an attack surface is "The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment" (2021).

Attack surfaces are the exposed areas that make systems more vulnerable to attacks and, essentially, is all the gaps in an organisation's security that could be compromised by a threat actor. This attack surface is increased through organisations incorporating things such as IoT technologies, migrating to the cloud and decentralising its workforce (Help Net Security 2021).

For many organisations, the pandemic forced a decentralisation of its workforce, as people had to work from home. For organisations who would usually have most, if not all, of its employees onsite – during the pandemic, these employees worked from home. These employees introduced new challenges because the attack surface widened to include every employee’s home internet connection (Forbes 2021; Recorded Future 2020).

6.1 Reducing the Digital Attack Surface

A digital attack surface can be described as everything on a network that is accessible through the internet. In particular, it includes those devices on the edge or outside of an organisation’s firewall (Tunggal 2021). The digital attack surface could include things such as cloud infrastructure, web applications, virtualization through container networking, industrial control systems and enterprise IoT. In addition, the digital attack surface includes endpoint devices on the edge of the network, such as mobile devices, laptops and desktop computers, that have access to internal resources, as well as access to the internet.

There are a variety of ways in which an organisation can protect itself from attack vectors on the digital attack surface and the responsibility for this usually lies with a dedicated, or integrated, IT security team. According to NIST’s Framework for Improving Critical Infrastructure Cybersecurity, the IT security team must identify assets and threats, protect an organisation’s information system infrastructure, be able to detect anomalies and attacks, respond to those attacks through detailed incident response strategies and to be able to recover by ensuring the resilience of the network to internal or external threats (2018).

There should be detailed network security policies and procedures in place to guide the IT security team on how to protect the network infrastructure and devices, which may include conducting penetration testing to find the vulnerabilities in a network, updating and patching relevant software and applications, shutting down unused ports, using a zero-trust security strategy and ensuring that only authorised people have access, both digital and physical, to secured areas.

However, very often the focus of cybersecurity is on these digital aspects or technical solutions – which include firewalls, intrusion detection and prevention, virtual private networks and encryption. Often people do not realise the dangers of clicking on unverified links and opening random attachments, or giving out information to anyone who requests it. Employees may assume that an organisation can protect itself from cyberattacks and that the security technologies are enough. However, while technology can filter out most attacks, it cannot eliminate everything (Roohparvar 2021). Therefore, people should be part of cybersecurity solutions and the human aspects of cybersecurity are important. These human aspects relate to the attitudes, perceptions, beliefs and behaviour of people within the context of cybersecurity, as well as how people can be influenced to intrinsically behave in a secure manner when online (Thomson 2010; Furnell & Thomson 2009; Joinson & Van Steen 2018).

6.2 Reducing the Human Attack Surface

If the human aspects of cybersecurity are neglected, the human attack surface is increased. The human attack surface is all the gaps and vulnerabilities created through the actions and activities of people. This could include negligence, errors, insider threats and the susceptibility of people to social engineering (Informer 2021; Tripwire 2017).

Social engineering attacks are targeted at people and rely on the psychological manipulation of people and social interaction to influence people to perform certain actions, such as click on a link, or divulge confidential information that benefits the threat actor. It is often referred to as ‘hacking the human’ and social engineers know that it’s a basic human instinct to trust something that looks legitimate – and anyone is susceptible (Thomson 2021; Peltier 2006).

Further, according to Verizon’s Data Breach Investigations Report, over three quarters of successful data breaches in 2020 had some element of defrauding humans, at least in the initial attack vector, rather than exploiting flaws in computer code or device configurations (2021).

Two examples of social engineering attacks took place in 2020. In South Africa in August, a company called Experian, a credit reporting agency, suffered a major data breach. Experian indicated that their IT infrastructure had not been compromised, but someone had ‘spoofed’ the company by posing as a client and supplied Experian with the names, surnames and identity numbers of millions of South Africans. This fraudulent client then asked Experian for data to complete these people's profiles – including home addresses, places of work and job titles, cell phone numbers and email addresses. The South African Banking Risk Information Center, or SABRIC, estimated over 24 million South Africans and almost 800 000 businesses were affected by this data breach (SABRIC 2020, Dlamini 2020).

Further, in July 2020, the official Twitter accounts of over 100 celebrities were hijacked by threat actors. These threat actors sent out messages to the celebrities' millions of followers, promising that they would double any Bitcoin sent to the address in the tweet and send it back to the donator. The followers had 30 minutes to click on the link to double their Bitcoin. Celebrity accounts hijacked included Barack Obama, Elon Musk, Jeff Bezos and Bill Gates, as well as organisations such as Apple and Uber – amongst many others. Within the space of a few hours, more than $100 thousand dollars' worth of Bitcoins had been transferred to the threat actor's Bitcoin wallet.

Twitter later tweeted that they had detected what appeared to be a coordinated social engineering attack on a few of their employees who had access to certain internal controls and tools, which gave the threat actors the ability to hijack the genuine Twitter profiles of these celebrities. It was later confirmed that a targeted phone spear phishing attack had been used (NPR 2020; Hansen 2020).

Humans are often spoken about as the 'weakest link' in the cybersecurity chain. However, the author believes that this mindset must be changed from seeing people as a risk that must be mitigated and to rather view them as part of the cybersecurity defense – a human firewall. In doing so, the human attack surface can be reduced. One of the best ways for an organisation to reduce the human attack surface is to cultivate a cybersecurity culture.

7. Cybersecurity Culture

A cybersecurity culture refers to the "knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies" (ENISA 2018).

The cultivation of a cybersecurity culture begins with, but must go beyond cybersecurity awareness. Learning is a continuum that starts with awareness, moves to training and evolves into education (NIST 2020).

Within the context of cybersecurity, the purpose of a cybersecurity awareness program should be to discuss 'what' cybersecurity is and to focus employees' attention on cybersecurity. Employees usually play a passive role as recipients of information, and it should lead to the recognition of cyberthreats and the retention of foundational cybersecurity information (NIST SP 800-16 1998).

A cybersecurity training program should communicate to employees 'how' they can protect themselves. It should build knowledge and give employees the necessary skills to successfully defend against cyberattacks. And there should be different levels of training – beginner, intermediate and advanced – linked to the roles and responsibilities of employees (NIST SP 800-16 1998).

A cybersecurity education program should enhance the insight of employees as to 'why' the skills they learnt through the Training Program are necessary. The learning objective of a cybersecurity education program is a comprehensive understanding of cybersecurity practices and procedures (NIST SP 800-16 1998).

Further, it is through this deeper insight and understanding that the attitudes and beliefs of employees, with regard to cybersecurity, start evolving and contribute to the cultivation of a cybersecurity culture, which should influence the day-to-day behaviour of employees to be aligned with security policies.

There are three levels of corporate culture – Artifacts, Espoused Values and Shared Tacit Assumptions (Schein 1999). Artifacts represent the observable behaviour and actions of people in an organisation. Espoused Values are those values supported by an organisation. The Shared Tacit Assumptions are the attitudes, beliefs and perceptions of people in the organisation (Schein 1999).

To contextualise this to a cybersecurity culture – the Espoused Values of an organisation should be expressed through the information or cybersecurity policies that should outline the expected behaviour of employees with regard to cybersecurity. Through cybersecurity awareness, training and education programs, these policies, and the importance of adhering to them, should be communicated to employees and ultimately positively influence their attitude, beliefs and perceptions with regard to cybersecurity. This would directly influence the cybersecurity-related behaviour of employees. Only when these three levels of culture align, when employees truly understand and fulfil the role they should be playing in cybersecurity, that a cybersecurity culture would have been cultivated (Thomson 2008).

While the cultivation of a cybersecurity culture in organisations is important, employees of organisations are not the only people going online. Many young children, teenagers, students, adults and retirees are using technology as part of their daily lives.

In 2015, the South African National Cybersecurity Policy Framework (NCPF) was proposed, in which it is said "To effectively deal with Cybersecurity, it is prudent that civil society, government and the private sector play their part in ensuring South Africa has a culture of Cybersecurity. Critical to this is the development of a culture of Cybersecurity, in which role players understand the risks of surfing in cyberspace" (National Cybersecurity Policy Framework 2015). This Framework clearly outlines the space and need for a national or a societal cybersecurity culture.

8. The Digital Footprint

As individual members of a society, individual users of technology should have an awareness of cybersecurity, as well as the skills required to safely navigate the online environment – and just as organisations have their attack surfaces, so too do individuals. However, the individual attack surface is more commonly called a digital footprint.

A digital footprint is a trail of data you create while using the internet and includes all digital traces, for example, the websites visited, emails sent, and information you submit to online services (Gervais 2018). There are both passive and active ways in which a digital footprint is created. A 'passive digital footprint' is a data trail left unintentionally, simply by being online. For example, when a website is visited, the web server may log an IP address, which identifies the ISP and approximate location of the user (Gervais 2018).

An ‘active digital footprint’ includes data that is intentionally submitted online. This includes tweets posted on Twitter, emails sent, status updates on Facebook and photos shared on Instagram, amongst a variety of other ways data is intentionally shared (Gervais 2018).

The so-called ‘Big Tech’ companies are collecting data on individuals all the time, including IP addresses, places of work, residences, interests and purchases. With this, they customise what gets advertised for users to click on; also known as ‘click-bait’ (Vigderman & Turner 2021).

In addition, there are data brokers who use data mining, and techniques such as information scraping, to collect and keep staggering amounts of personal information about consumers, including things like usernames, passwords, banking information and credit card details. Data brokers also rely on users to freely give away personal information in exchange for free services like apps and games. These data brokers then sell this information to anyone who is prepared to pay, including, for example, advertisers and marketers, political campaigns and prospective employers (Latto 2020). Further, even with robust data privacy laws, such as the GDPR in the European Union and POPIA in South Africa, there is still a vast amount of data that is collected. With all of this data being collected and stored, it only takes one data breach for cybercriminals to get hold of sensitive information.

Therefore, users need to reduce their individual attack surfaces when online – both the digital and human attack surfaces. Users should ensure their devices are as secure as possible. Further, users should be aware of how the tendency to trust may be exploited by social engineers, through things like phishing attacks.

8.1 Reducing the Individual Digital Attack Surface

With regard to their digital attack surface, users need to ensure they have the latest updates and patches for the software they are using, and firewalls and antivirus software should be installed and checked for updates often. This should be done on all the devices used to go online – including smartphones, computers or any IoT devices (Klosowski 2019).

Further to this, users need to ensure that they use the security and privacy settings on social media accounts and use anti-tracking software and freely available anti-tracking browser extensions. In addition, multifactor or two-factor authentication, which uses, in addition to a password, another factor for authentication should be activated on services such as Facebook, WhatsApp, Google and Instagram (Klosowski 2019). While this is not an exhaustive list of all the possible ways users can reduce their digital attack surface, it does form part of basic cybersecurity recommendations.

8.2 Reducing the Individual Human Attack Surface

In addition to these technical measures to reduce their individual digital attack surface, users need to be aware of the ways in which threat actors may target them. Being able to recognise phishing and social engineering attacks is essential for operating securely online. This is often easier said than done, as there are such a variety of ways in which people are targeted. However, there are ‘red flags’ that could alert users to possible phishing attacks (IT Governance 2020).

Users need to check, not just who an email is coming from, but which email address it is coming from. Very often phishing emails come from public email domains, like Gmail or Yahoo, or the domain name is misspelt. Phishing emails are typically poorly written – however, with spear phishing attacks, where particular people are targeted, or Business Email Compromise attacks – these messages are crafted to look more genuine (Federal Trade Commission 2019).

Further, if there is an active link or an attachment to click on in any communication received, users should be cautious and ensure that the communication is from someone trustworthy. If anything about an email or message seems suspicious, users should find an alternate way to contact the person who supposedly sent the email (IT Governance 2020). It is further recommended that users check where links will take them before clicking on the links. Users should use their mouse to hover over the link and, if there is a mismatch between where the link appears to be from and where it actually goes, users should not click the link. A further 'red flag' would be a sense of urgency or a limited time offer. This is very often indicative of phishing attacks, as threat actors know that if users have time to think, there is a greater chance that they may identify something suspicious (IT Governance 2020; Federal Trade Commission 2019).

There are a large variety of other types of social engineering attacks and users should be cautious of anyone requesting information and should verify who they are communicating with – and, in this way, reduce the individual human attack surface.

9. A Cybersecurity Conscious Society

In order for users to be able to reduce their attack surface, they must be cybersecurity aware. From a societal cybersecurity culture point of view, there should be coordinated cybersecurity awareness programs and campaigns for all people going online, including, young children, teenagers, students and adults.

These cybersecurity awareness campaigns need to be both appropriate for various age groups, as well as the various environments in which people operate. Further, these cybersecurity awareness programs and campaigns should be targeted to the particular threats relevant to a particular group. For example, parents of young children should be made aware of the threats their children may be exposed to online and how to protect them, teachers and lecturers should make students aware of the basics of cybersecurity, including aspects such as cyberbullying and netiquette, and the government, private sector and public sector should all be key stakeholders in raising cybersecurity awareness to create users who are not only confident and capable online, but who can operate securely online, as well.

Further, the cybersecurity awareness campaigns should be underpinned by behavioural theories, such as Social Learning Theory, Sociocultural Theory and the Protection Motivation Theory, together with pedagogically sound educational principles – to translate cybersecurity awareness into action. Therefore, the approach and the way forward for cultivating a societal cybersecurity culture is truly interdisciplinary.

10. Conclusion

As the world becomes more and more interconnected, with more and more users online, security is often not seen as a priority. In addition to the creation of cybersecurity cultures within organisations, individual users should play a role in cybersecurity awareness. Each person needs to play a role in cybersecurity awareness, and to make it a priority to be proactive against cyberattacks, instead of reactive. Not everyone needs to be a cybersecurity expert, but all should be working together to create a society that is cybersecurity conscious.

Through this cybersecurity conscious society, both the digital and human attack surfaces can be reduced and the benefits that technology has to offer can be realised in our interconnected world.

References

Aeris. 2021. IoT in Commercial Aviation [Online]. Available at: https://www.aeris.com/news/post/iot-in-commercial-aviation/ [accessed 17 May 2021]

Calo, S.B., Touna, M., Verma, D.C., Cullen, A., 2017. Edge computing architecture for applying AI to IoT. In 2017 IEEE International Conference on Big Data. Boston, MA, USA 11-14 December 2017. IEEE: New Jersey.

De Silva, A., 2017. Fog Computing [Online]. Available at: https://www.terminalworks.com/blog/post/2017/05/13/fog-computing [accessed 10 August 2021].

Dlamini, S., 2020. Data breach at Experian, 24 million South African's personal information exposed. [Online]. Available at: https://www.iol.co.za/business-report/economy/data-breach-at-experian-24-million-south-africans-personal-information-exposed-342b8690-f43c-4657-8555-5b55b099418a [accessed 20 May 2021]

Dorsemaine, B., Gaulier, JP., Wary, JP., Kheir, N, 2015. Internet of Things: A Definition & Taxonomy. In 9th International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST. Cambridge, United Kingdom 9-11 September 2015. IEEE: Germany.

ENISA, 2018. Cyber Security Culture in Organisations. [Online]. Available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations [accessed 22 July 2021]

Federal Trade Commission, 2019. How to Recognize and Avoid Phishing Scams. [Online]. Available at: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams [accessed 26 June 2021]

Fontanilla, M.V., 2020. Cybercrime Pandemic. Eubios Journal of Asian and International Bioethics. [Online]. 30 (4), Available at: https://www.eubios.info/EJAIB52020.pdf#page=33 [accessed 2 August 2021]

Forbes, 2019. What Is The Artificial Intelligence Of Things? When AI Meets IoT [Online]. Available at: https://www.forbes.com/sites/bernardmarr/2019/12/20/what-is-the-artificial-intelligence-of-things-when-ai-meets-iot/?sh=53e5d12db1fd [accessed 27 July 2021]

Forbes, 2021. Your Growing Digital Attack Surface And How To Protect It. [Online]. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/07/23/your-growing-digital-attack-surface-and-how-to-protect-it/?sh=18d942373194 [accessed 31 July 2021]

Fruhlinger, J., 2020. What is phishing? How this cyber attack works and how to prevent it. [Online]. Available at: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html [accessed 29 March 2021]

Furnell, S., Thomson, K., 2009. From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud & Security, [Online]. 2009 (2), Available at: https://www.sciencedirect.com/science/article/abs/pii/S1361372309700193?via%3Dihub [accessed 8 June 2021]

Gervais, J., 2018. What is a digital footprint? And how to help protect it from prying eyes. [Online]. Available at: https://us.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html [accessed 2 June 2021]

Hansen, C., 2020. Hackers Hijack Twitter Accounts of Obama, Biden, Kayne West, Apple and Others. [Online]. Available at: https://www.usnews.com/news/national-news/articles/2020-07-15/hackers-hijack-twitter-accounts-of-barack-obama-joe-biden-kayne-west-apple-and-others [accessed 2 August 2021]

Help Net Security, 2021. Corporate attack surfaces growing concurrently with a dispersed workforce. [Online]. Available at: https://www.helpnetsecurity.com/2021/06/16/corporate-attack-surfaces/ [accessed 21 June 2021]

Hootsuite, 2021. The Global State of Digital 2021. [Online]. Available at: https://www.hootsuite.com/resources/digital-trends [accessed 30 July 2021]

Hummel, R., Hildebrand, C., 2021. Crossing the 10 Million Mark: DDoS Attacks in 2020 [Online]. Available at: https://www.netscout.com/blog/asert/crossing-10-million-mark-ddos-attacks-2020 [accessed 4 April 2021]

IBM Security, 2021. Cost of a Data Breach Report 2021. [Online]. Available at: https://www.ibm.com/downloads/cas/OJDVQGRY [accessed 4 August 2021]

Informer, 2021. The Human Attack Surface - A Serious Threat to Cyber Security. [Online]. Available at: https://www.informer.io/resources/the-human-attack-surface-a-serious-threat-to-cyber-security [accessed 9 May 2021]

IT Governance, 2020. 5 ways to detect a phishing email – with examples. [Online]. Available online: https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email [accessed 4 June 2021]

Joinson, A., Van Steen, T., 2018. Human aspects of cyber security: Behaviour or culture change? Cyber Security: A Peer-Reviewed Journal, [online]. 1 (4), Available at: https://hstalks.com/article/3262/human-aspects-of-cyber-security-behaviour-or-cultu/ [accessed 12 June 2021]

Joyia, G.J., Liaqat, R.M., Farooq, A., Rehman, S., 2017. Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain. *Journal of Communications*, [online]. 12 (4), Available at: http://www.jocm.us/uploadfile/2017/0428/20170428025024260.pdf [accessed 7 August 2021]

Landi, H., 2019. Report: 40% of healthcare organizations hit by WannaCry in past 6 months. [Online]. Available at: https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months [accessed 10 April 2021]

Klosowski, T., 2019. How to Protect Your Digital Privacy. [Online]. Available at: https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy [accessed 27 June 2021]

Lastdrager, E.E., 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, [online]. 3 (9), Available at: https://crimesciencejournal.biomedcentral.com/track/pdf/10.1186/s40163-014-0009-y.pdf [accessed 3 April 2021]

Latto, N., 2020. Data Brokers: Everything You Need to Know. [Online]. Available at: https://www.avast.com/c-data-brokers [accessed 9 July 2021]

Martech Advisor. 2019. By 2030, Each Person Will Own 15 Connected Devices — Here's What That Means for Your Business and Content [Online]. Available at: https://www.martechadvisor.com/articles/iot/by-2030-each-person-will-own-15-connected-devices-heres-what-that-means-for-your-business-and-content/ [accessed 5 August 2021]

McAfee, 2021. ATR Threats Report [Online]. Available at: https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html [accessed 1 June 2021]

National Cybersecurity Policy Framework, 2015. South African Government Gazette.

NIST SP 800-16, 1998. Information Technology Security Training Requirements:
A Role- and Performance-Based Model. [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [accessed 4 August 2021]

NIST. 2018. Framework for Improving Critical Infrastructure Cybersecurity. [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [accessed 5 May 2021]

NIST, 2020. Awareness, Training, & Education. [Online]. Available at: https://csrc.nist.gov/projects/awareness-training-education [accessed 8 August 2021]

NIST, 2021. Computer Security Resource Center Glossary. [Online]. Available at: https://csrc.nist.gov/glossary/term/attack_surface [accessed 16 May 2021]

NPR, 2020. Twitter Says It Was the Victim of a 'Coordinated Social Engineering Attack'. [Online]. Available at: https://www.npr.org/2020/07/15/891614274/twitter-accounts-of-jeff-bezos-bill-gates-joe-biden-barack-obama-hit-by-hackers [accessed 2 August 2021]

Palmer, D., 2021. Ransomware as a service is the new big problem for business. [Online]. Available at: https://www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/ [accessed 28 March 2021]

Pascariu, C., Barbu, I., 2015. Ransomware - an Emerging Threat. *International Journal of Information Security and Cybercrime (IJISC)*, [online]. 4 (2), Available at: http://www.ijisc.com/articles/2015-02-03.pdf [accessed 12 June 2021]

Patel, K. and Patel, S., 2016. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineering Science and Computing*, [online]. Available at: http://www.opjstamnar.com/download/Worksheet/Day-110/IP-XI.pdf [accessed 5 August 2021]

Peltier, T.R., 2006. Social Engineering: Concepts and Solutions. Information Systems Security, [online]. 15 (5), Available at: https://www.researchgate.net/publication/220450160_Social_Engineering_Concepts_and_Solutions [accessed 15 June 2021]

Recorded Future, 2020. Remote Threats to Remote Employees: How Working From Home Increases the Attack Surface. [Online]. Available at: https://www.recordedfuture.com/remote-attack-surface/ [accessed 18 June 2021]

RiskBased Security, 2020. 2020 Year End Report - Data Breach QuickView. [Online]. Available at: https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf [accessed 16 May 2021]

Robles, R.J., Kim, T., 2010. Applications, Systems and Methods in Smart Home Technology: A Review. *International Journal of Advanced Science and Technology*, [online]. 15, Available at: https://www.researchgate.net/profile/Rosslin-Robles/publication/311414479_Applications_Systems_and_Methods_in_Smart_Home_Technology_A_Review_IJAST_vol15/links/584501b908aeda6968191835/Applications-Systems-and-Methods-in-Smart-Home-Technology-A-Review-IJAST-vol15.pdf [accessed 7 August 2021]

Roohparvar, R., 2021. People - the Weakest Link in Cybersecurity. [Online]. Available at: https://www.infoguardsecurity.com/people-the-weakest-link-in-cybersecurity/ [accessed 17 April 2021]

SABRIC, 2020. Experian Data Breach. [Online]. Available at: https://www.sabric.co.za/media-and-news/press-releases/experian-data-breach/ [accessed 5 June 2021]

Schein, E.H., 1999. The corporate culture survival guide. San Francisco, California, United States of America: Jossey-Bass Publishers.

Statista. 2021. Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 [Online]. Available at: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ [accessed 10 May 2021]

Thomson, K., 2008. MISSTEV: Model for Information Security Shared Tacit Espoused Values. DTech. Nelson Mandela Metropolitan University

Thomson, K., 2010. Information Security Conscience: a precondition to an Information Security Culture? *Journal of Information System Security*. 6 (4) Available at: https://www.jissec.org/Contents/V6/N4/V6N4-Thomson.html [accessed 10 April 2021]

Thomson, K., 2021. Social Engineering. In: Jajodia S., Samarati P., Yung M. (eds) Encyclopedia of Cryptography, Security and Privacy, [online]. Available at: https://doi.org/10.1007/978-3-642-27739-9_1593-1 [accessed 1 June 2021]

Tripwire, 2017. The Human 'Attack Surface' May Be Your Weakest Link Available at: https://www.tripwire.com/state-of-security/ics-security/human-attack-surface-may-weakest-link/ [accessed 10 May 2021]

Tunggal, A.T., 2021. What Is an Attack Surface? Tips to Reduce Your Attack Surface. [Online]. Available at: https://www.upguard.com/blog/attack-surface [accessed 10 August 2021]

Verizon, 2021. Data Breach Investigations Report. [Online]. Available at: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ [accessed 4 July 2021]

Vigderman, A., Turner, G., 2021. The Data Big Tech Companies Have On You. [Online]. Available at: https://www.security.org/resources/data-tech-companies-have/ [accessed 22 June 2021]