The Journal of Supercomputing
https://doi.org/10.1007/s11227-019-03028-9

Threats on the horizon: understanding security threats in the era of cyber-physical systems

Steven Walker-Roberts[1] · Mohammad Hammoudeh[1] · Omar Aldabbas[2] · Mehmet Aydin[3] · Ali Dehghantanha[4]

Abstract

Disruptive innovations of the last few decades, such as smart cities and Industry 4.0, were made possible by higher integration of physical and digital elements. In today's pervasive cyber-physical systems, connecting more devices introduces new vulnerabilities and security threats. With increasing cybersecurity incidents, cybersecurity professionals are becoming incapable of addressing what has become the greatest threat climate than ever before. This research investigates the spectrum of risk of a cybersecurity incident taking place in the cyber-physical-enabled world using the VERIS Community Database. The findings were that the majority of known actors were from the US and Russia, most victims were from western states and geographic origin tended to reflect global affairs. The most commonly targeted asset was information, with the majority of attack modes relying on privilege abuse. The key feature observed was extensive internal security breaches, most often a result of human error. This tends to show that access in any form appears to be the source of vulnerability rather than incident specifics due to a fundamental trade-off between usability and security in the design of computer systems. This provides fundamental evidence of the need for a major reevaluation of the founding principles in cybersecurity.

Keywords Cyberattacks · Cyber defence · Cyber-physical systems · VERIS · VCDB

✉ Mohammad Hammoudeh
M.Hammoudeh@mmu.ac.uk

Steven Walker-Roberts
s.walkerroberts@mmu.ac.uk

1 Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK

2 Faculty of Engineering, Al-Balqa' Applied University, As-Salt, Jordan

3 Department of Computer Science and Creative Technologies, University of the West of England, Bristol, UK

4 School of Computer Science, University of Guelph, Guelph, ON, Canada

Published online: 24 October 2019

1 Introduction

The Internet of Things (IoT) revolution led to an exponential increase in the number of physical things that are connected to the Internet [23]. IoT and other connected data technologies, i.e. cyber-physical systems (CPS), thrive to enhance existing infrastructure and operational systems. CPS can bring a number of benefits to citizens, business and governments. However, securing these systems in a piecemeal mode has proven a monumental challenge [5]. With the continuous implementation of time- and safety-critical applications of CPS, the security risks and costs of potential attacks will continue to grow. As core components of safety-critical infrastructures, CPS, e.g. smart grid, have become an attractive target for cyberattacks. To illustrate, hackers sabotaged the control system of Ukraine's electric grid causing power outage affecting about 230,000 people. Without effective security controls, attackers are potentially able to access a CPS, sometimes using Internet connected devices as an entry gateway, causing damage from long distances [17].

Cybersecurity has rapidly become an issue of major contemporary relevance in computer science. With cybersecurity incidents increasing every year, the state of the art has only become more apparent as deficient [12, 30, 31]. It is important that whilst the trend does appear to be an increasing frequency and seriousness of cybersecurity incidents, it remains an area of study which is often misunderstood and highly controversial. In many cases, cybersecurity technologies, data and heuristic methods are proprietary and unavailable for academic observation or use for free by those less economically able but whom the literature recognises as being the most vulnerable to cybersecurity incidents [6]. Thus, the long-term sustainability of day-to-day computing technologies is questionable. For example, Heartbleed [13], a vulnerability potential affecting the whole Internet, could not have been avoided because even a small human error can have catastrophic consequences. In that case, it was a short-spanned programming error many years earlier, but its effect was catastrophic. The likelihood of some influence on security leading to a breach is a matter of chance resulting from the methods used in computer security, primarily the heuristic nature of computer security software.

The majority of cybersecurity incident datasets are proprietary, often coupled with the added caveat that when vulnerabilities are discovered they are either kept secret or are only shared within acutely technical circles. Consequently, before and during the vulnerability discovery phase there is an opportunity presented for potentially silent zero-day exploitation by attackers who could be extremely capable.

It can therefore be argued that in reality, the focus is not on the nature and content of an exploit specifically, but how it is able to weave between computer security structures to achieve the end goal of exploitation. Thus, the objective of this research is to understand the risks and niceties of the largest publicly available dataset of cybersecurity incidents with the overall aim to identify patterns of importance among the dataset, particularly ones that are CPS specific. This is achieved by studying the characteristics of the VERIS Community Database (VCDB) of cybersecurity incidents. VCDB is the most accepted open-source dataset for cybersecurity incidents in industry, academia and government [16]. It records a number of

cybersecurity incident features, some of which are attack mode, actor type, impact, victim type, timeline and prose summaries often accompanied by a hard reference to a source. The dataset, as of writing, now contains about 7000 unique incidents gleaned from real-life data breaches over a period of 12 years [26]. The existing VCDB dataset has extensive fielding, which is appropriate in degree to extensively critically analyse the mechanisms of cybersecurity incidents. Other datasets are too specific and do not provide a temporal dimension to security incidents.

The general trend within cybersecurity is for each organisation to take a different stance by using a different analytics platform to record cybersecurity incidents and data breaches. Indeed, cybersecurity risk analytics has become a lucrative venture [15]. This is unhelpful because not only is the data relating to cybersecurity incidents not reaching a central information repository which other users can benefit from, the organisations themselves may implement means and models which are not particularly effective nor accurate.

The motivation for this research is to analyse in detail the largest and most comprehensive dataset available for cybersecurity incidents in order to understand a greater depth of context to cybersecurity incidents. The objective is to, by Monte Carlo simulation, map a range of possibilities for future attack modes. An added motivation is to create a model for a repeatable approach to analysis of this dataset (VCDB) and other cybersecurity incident datasets. The model for the approach in this research is repeatable in other research studies.

The rest of the paper is organised as follows: Sect. 2 gives the key threats to CPS and the motivation behind this research. Section 3 covers recent studies that attempt to analyse data breaches. Section 4 details our methodology for feature analysis and the Monte Carlo simulation. Section 5 details the results of risk modelling. In Sect. 6, the results are thoroughly analysed with respect to frequency, increasing rate and loss, the principles of least privilege, human error and criticality. Section 7 concludes the paper and identifies future work avenues.

2 CPS security threats and motivation

The cybersecurity risks in CPS have become a serious concern for security professionals. This is particularly true as CPS is increasingly deployed in critical infrastructure, manufacturing and everyday life such as building control, medical devices and smart grid. When a connected endpoint is breached, a backdoor into other parts of the network is created. Hence, the result of malicious attacks can have severe consequences on human lives, business productivity and national security. In the following, we highlight some of the key security threats to CPS; we refer interested readers to the following works [3, 5, 9, 20, 32] for an extensive treatment of the topic.

Industry is driven by functional requirements with little attention to security. The massive growth in the number of CPS connected devices increases the attack vector. Most of these devices have long lifespans. Many devices do not get enough security updates; some never get updated at all. This is partially due to the fact that a CPS device has been managed by operational technology teams rather than IT

departments leading to excluding them from the proactive and coordinated efforts that are deployed to secure enterprise systems.

CPS device are at risk of being compromised for various reasons. Some, often heuristic, attacks could hijack connected devices and turn them into email servers for mass spam, use them as botnets for executing DDoS (Distributed Denial of Service) attacks or simply cause interruption to business processes. The motivation behind these attacks could be financial, e.g. tamper with a physical utility meter or inject false data to misinform the production process causing monetary loss. Many attacks are also motivated by political reasons such as interrupting power supply as part of cyber warfare.

The limited computation, communication and processing resources of common CPS devices make the application of classical data encryption and secure communication protocols impractical. Hence, many CPS devices do not encrypt communication between devices and with the cloud servers. Secure communication protocols must be used to protect against unsafe communication. More recently, with the rising popularity of the zero trust security model, micro-segmentation is used to assign CPS devices to a separate network to create private communication that keeps the transmitted data secure.

One of the common CPS vulnerabilities is the use of default passwords and device misconfiguration. Until today, most devices are shipped with default passwords and settings. Attackers can use this knowledge to brute force into these devices. Weak credentials put both the user and their business at risk of being susceptible to attacks. After gaining access to CPS devices, attackers can establish remote sessions and use them to monitor the owners without their knowledge. Furthermore, attackers can use CPS devices, either through their IP addresses or built-in GPS chip, to find a user's physical location. Installing a VPN to secure a CPS can keep the IP address private. As CPS connects the physical and virtual worlds, unsecured devices which for instance are part of a home security system, when compromised can cause massive risks to personal and business safety. One of the examples of remote access attacks is hijacking self-driving vehicles and even asking the owners to pay a ransom to return control of the vehicle, machine or medical device.

In conclusion, the plethora of different CPS devices brings various vulnerabilities. New trends such as the use of artificial intelligence (AI) and automation introduce a new vector of security threats to CPS. In modern AI-enabled CPS, simple coding errors can bring down the entire infrastructure that it was controlling. The human factor plays a key role in securing CPS; this threat can be resolved through educating individuals using or managing a CPS. Education goes beyond technical knowledge of how to secure a system to cover awareness about the impact of CPS and security attacks, which could be the difference between having a secure network and a security breach. The scale and complexity of a CPS system makes it expensive and time-consuming to secure CPS infrastructure. Security threats for CPS are only expected to intensify as more targets are becoming available. With the rise of Industry 4.0, machine phishing will become a serious concern to the smart manufacturing sector. Manufacturers and other CPS users will have to invest more in addressing the serious security vulnerabilities and threats. This paper is set to identify imminent security threats to CPS and beyond. We believe that understanding the sources of

threats is the first line of defence against such risks as it helps organisations implement their information security strategies, make well-informed governance decisions and mitigates risks at an early stage.

3 Related work

There is a recognised sparsity of complete incident datasets for cybersecurity [19]. Comparisons of various datasets have been performed, but this has not included a detailed consideration of the underlying scientific and social mechanisms of cybersecurity incidents [14]. The demand for research conducting data breach analysis is very well recognised; nonetheless, there appears to be a general sparsity within the literature of such works, particularly more searching research [1].

There are very recent and rigorous research papers which analyse data security breaches [4]. The authors of [31] ascertain the existing technological capability to mitigate insider threats within computer security systems by way of a mixed-method systematic review. This research does not take into account the malicious insider. In [21], a systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment is conducted.

Such research efforts do not investigate the wider temporal dimensions of these breaches but instead focus on common mechanisms. There is clearly a demand for research investigating wider perspectives. This motivates our research to understand the nature of security threats so that new technologies can be developed around potential further findings.

4 Feature analysis and Monte Carlo simulation methods

The approach in this study was complex and time-consuming owing to the need to manually sort data. Data was downloaded from the vz-risk/vcdb [26] repository in JSON format and the schema analysed using purpose-built software. A software package "VerisDB Analyst" was created to parse that JSON data and present it both in a web application and a REST API over HTTP [29]. The analysis conducted by the application was performed through MapReduce functions [11], which appear in and are explained by [27]. VerisDB Analyst is backed by a MongoDB database. In this particular study, the software was tested against MongoDB Atlas (the cloud offering of MongoDB) and was tested against a local installation. The primary reason for this was to assess connection and database drop-outs.

The VerisDB Analyst application contains the MapReduce function in Algorithm 1. That MapReduce algorithm was implemented in respect of each type of property [27]. The algorithm was slightly tailored to the properties in the VERIS schema [26] because it does not presently adhere to the JSON specification [7] since some keys and values are arbitrarily stored in sub-objects and property names. This posed challenges for parsing the data, because the data heirarchy was sophisticated by those problems. As a direct consequence, the Javascript used to make VerisDB Analyst is not optimal. It could be argued that data should have

been pre-corrected, but this approach was not taken because VERIS is open-source and it was more appropriate to raise it as an issue with the Verizon RISK team [28].

Algorithm 1 MapReduce Algorithm derived from [11]

```
function MapProps(jsonAray)
    mappedObject = {}
    for jsonObject ∈ jsonArray do
        p ← convert(jsonObject.prop)
        p → mappedObject
    end for
return mappedObject
end function
function ReduceProps(jsonMap)
    reducedObject = {}
    for jsonObject ∈ jsonMap do
        key ←  (jsonObject.key)
        value ← Σ (jsonObject.prop)
        keys[] ← key
        values[] ← value
        keys, values → reducedObject
    end for
return reducedObject
end function
```

The purpose of Algorithm 1 was to extract only the relevant data for the purposes of summarising the cybersecurity incident data. Only the overlying trends were important, not the structure or metadata of the database state itself (in this case a JSON tree). The algorithm was performed in Javascript ES7 in node.js 8.8.1. The algorithm returned computations in respect of whole objects summarised from the whole JSON database as stored on MongoDB within 2441 ms on an Intel i3-4030 single-threaded 8GB RAM on a commodity HP G6 laptop repurposed as a server which runs the LXD container platform. The application used for statistical analysis was held in a container with MongoDB 3.4 installed locally. Given that the JSON database is 19 MB and was processed around 5 times through MongoDB aggregation queries, this is a satisfactory return time though it could be greatly enhanced with some further optimisations. Present reducibility is 75% with 19 MB reduced to 4.75 MB.

Data was extracted using the VerisDB Analyst web application which analyses the whole dataset on the fly. The match property used is the MongoDB 3.4 implementation of $match, which contains an evaluation to be performed which has to be satisfied for documents to be returned. For example, this could be whether a specified property condition is true. The group property is simply a string representation of a property to be aggregated and counted using a standardised query structure. This uses the MongoDB 3.4 implementation of $group. The sort property contains a sub-object with a single key, value pattern. The key is the property to sort against, the integer value indicated whether to sort in ascending or

descending order. The unwind property flattens arrays in the specified property path in the JSON hierarchy.

5 Risk assessment modelling results, summarised data fields

Figure 1 shows the results of the Monte Carlo simulation. The results were obtained for each type of query using the VCDB Dataset as at 20 October 2017. Data was obtained for actors, attack mode, the impact of any attacks and victim demographics. It should be noted that not all entries within the VCDB dataset report on all incident information. Thus, some incidents may have contained information on one field of interest but not on others, e.g. might report attack data but not victim data.

Any reference to banding within this section means a group of the highest figures, which when taken together in a group or "band", have central tendency. The

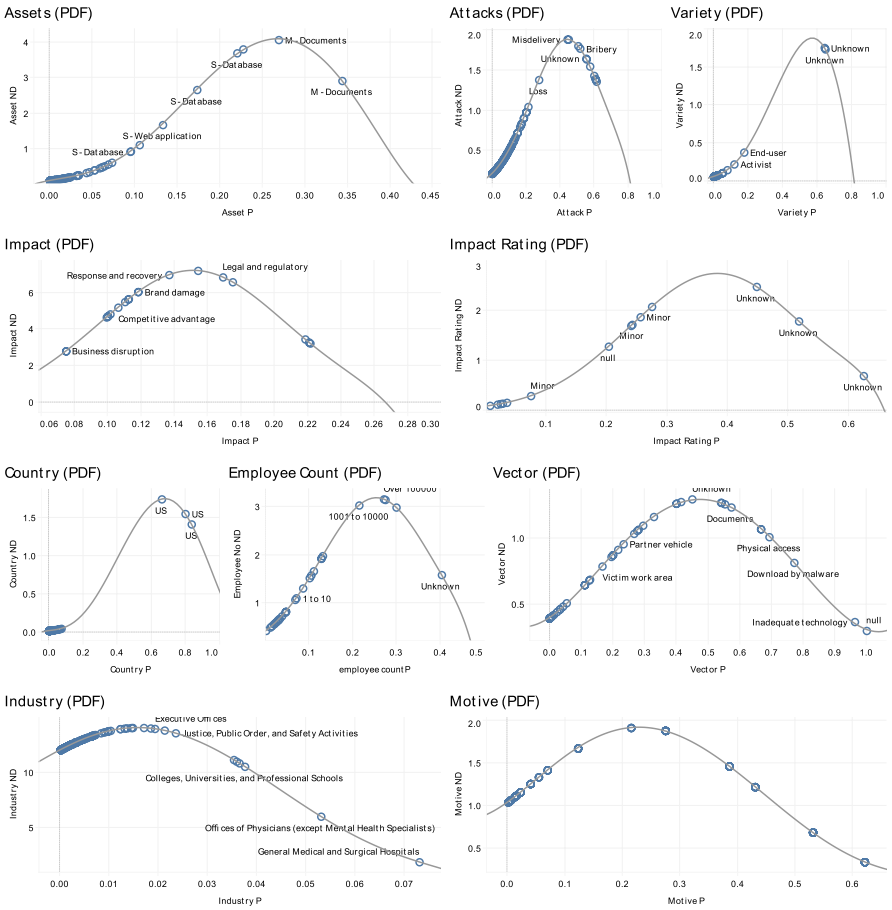

Fig. 1 The results of the Monte Carlo simulation

central tendency was not significant of itself but represents two caveats: (i) a collection of similar occurrences may show central tendency because multiple collection fields could refer to the same overall field (a global field) and (ii) the central tendency could reflect a probabilistic confidence interval owing to a characteristic of the dataset which may or may not have been inferential but where there are too many degrees of freedom to formally prove specific inference from data properties.

There appeared to be extensive data on actors within the VCDB dataset. The dataset relating to actors appeared in Table 1. The dataset showed remarkable features across all fields in respect of each actor type (internal, external or partner).

Internal actors tended to be motivated financially (602) compared to the external and partner actor groups. This was followed closely by the motivations of fun (200) which also featured strongly, corporate espionage (63), convenience (56) and grudges (48). In a large number of incidents, the motivation was not known (757). The dataset reported that in a large proportion of incidents the incidents were accidents (1703).

Figure 2 shows the actor type distribution. Typical actors were end-users (615) and system administrators (93) who featured in the strongest band. This was followed by executives (83), financiers (65), cashiers (57), managers (47) and developers (45) who were groups which lie in a similar band of prevalence.

Most external actors originated from the USA (219) and Russia (124) which were in the highest band. China (53), Pakistan (42), Great Britain (41) and Syria (38) form the second from highest band. The United Arab Emirates (30), Turkey (24) and North Korea (20) form the lowest band. There were (2975) records concerning external actors where the geographic origin of the attacker was not known.

The majority of actors were motivated financially (1480), by political or religious ideology or protest (367), espionage (266) and fun (211). In the 1242 incidents involving external attackers, the motive of the attacker was not known. External actors were primarily activists (468), independent attackers (311), state affiliated (209) or the attacks took place during the commission of wider organised criminal offences (198). There was a secondary band of similar prevalences, which consisted of former employees (57) and nation states (39). In 2538 incidents, the variety of external actor was not known.

The majority of incidents where the actor was a partner of the victim involved originators from the USA (104). This was followed by a much smaller band, consisting of Great Britain (9), India (5), Canada (4), Republic of Ireland (2) and Australia (2). In the majority of incidents involving partners, the geographic origin of the actor could not be established (213).

The majority of incidents involving partners were accidental or unintentional (179). This was followed by a strong banding of financial motivation. The majority of actor varieties could not be established and were recorded as unknown (143).

There was a considerable amount of data relating to attack modes within Table 2. The attacks were grouped into modes, namely error, hacking, misuse, physical, malware, social, unknown and environmental. The group featuring the largest number of incidents was the "error" (2038) group together with "hacking" (1927); these groups were relatively similar in value. The "misuse" (1409) and "physical" (1343) groups

Table 1 Actors data in the analysed VCDB dataset

Internal					External				
Motive	#	Variety	#	Country	#	Motive	#	Variety	#
NA	1703	Unknown	2239	Unknown	2975	Financial	1480	Unknown	2538
Unknown	757	End-user	615	US	219	Unknown	1242	Activist	468
Financial	602	Other	173	RU	124	Ideology	367	Unaffiliated	311
Fun	200	System admin	93	CN	53	Espionage	266	State-affiliated	209
Espionage	63	Executive	83	PK	42	Fun	211	Organised crime	198
Convenience	56	Finance	65	GB	41	Grudge	89	Former employee	57
Grudge	48	Cashier	57	SY	38	NA	28	Nation state	39
Other	37	Manager	47	UA	30	Other	16	Other	37
Ideology	11	Developer	45	TR	24	Secondary	8	Force majeure	19
Fear	3	Human resources	26	KP	20	Fear	3	Customer	15
		Call centre	14	CA	16	Convenience	1	Competitor	12
		Guard	8	IR	15			Acquaintance	10
		Helpdesk	8	RO	14			Terrorist	4
		Maintenance	7	IN	11			Auditor	2
		Auditor	4	AU	9				

Partner			
Country	#	Motive	#
Unknown	213	NA	179
US	104	Unknown	143
GB	9	Financial	37
IN	5	Convenience	5
CA	4	Espionage	5
IE	2	Fun	4
AU	2	Other	3
NZ	1	Grudge	1
BH	1		
JP	1		
KP	1		
PH	1		
IT	1		
DE	1		

formed a lower secondary banding of similar values. There was a much lower tertiary banding of the groups “malware” (545) and “social” (451). The banding was likely to be inferential to other fields.

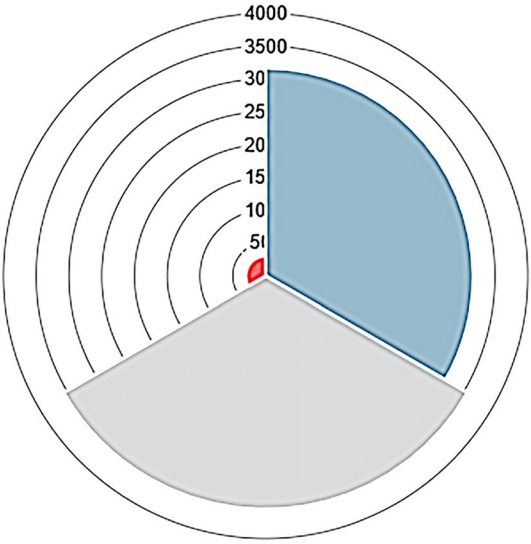

Fig. 2 Attack actor type distribution

Blue: Internal; Grey: External; Red: Partner

Figure 3 shows a summary of the attack discovery method. The sample reported in this study was taken from incidents involving hacking. In 797 cases, the means of discovery were not known. Over 559 incidents were voluntarily disclosed by the actors in question. There were 151 incidents identified as a result of suspicious traffic on the network. In 86 cases, the incidents were discovered when employees reported observations. In 73 cases, the customer reported observations which led to discovery of the incident in question. HIDS detection was apparent in only five cases involving hacking.

The incident rate per year appeared to be latent until the rate of change in incidents per year increased rapidly from 2009 (89) until 2010 (579)—this appeared as the first peak in Fig. 4. There was a fall in the incident rate in 2011 (537) after which there was a dramatic rate of change in incident rate, increasing from 1252 in 2012 to 1907 in 2013—this forms the second peak which appeared in Fig. 4. The rate of change almost entirely reversed to 2014 (902) and plateaued through to 2015 which stayed at a steady incident rate (862) and dropped lower to (649) in 2016.

The financial loss per year reported in the dataset followed a logarithmic scale as in Fig. 5. The rate of change was relatively inconsistent from year to year but with an exponential increase between 2015 and 2016. The year financial loss at 2016 was approximately 1e10 USD. The 2016 value was an exponential increase from previous years. From 2010 to 2015, there were exponential fluctuations in what appeared to closely resemble a sinusoidal function. The only exception to that sinusoidal function was in 2006 (9e3 USD) where there appeared to be an exponential decrease in the financial loss amount in that year when compared to other years in the function.

The results pertaining to impact variety are illustrated in Fig. 6. The largest impact of cybersecurity incidents was in assets and fraud (245), followed by

Table 2 Attack data in the analysed VCDB

Hacking					
Variety	#	Vector	#	Asset	
Unknown	1237	Web application	949	S—Web application	1059
Use of stolen creds	228	Unknown	713	S—Database	350
Use of backdoor or C2	195	Backdoor or C2	197	S—Unknown	287
DoS	152	Other	30	U—Desktop	238
Brute force	131	Physical access	13	P—Unknown	210
SQLi	99	Partner	10	Unknown	205
Abuse of functionality	31	Desktop sharing	10	N—Router or switch	99
Other	31	Command shell	8	U—Mobile phone	89
Forced browsing	14	VPN	5	S—Mail	59
MitM	8	3rd party desktop	2	U—POS terminal	27
XSS	6			S—POS controller	25
Buffer overflow	4			P—End-user	23
SSI injection	4			S—File	23
Physical					
Variety	#	Vector	#	Asset	
Theft	1041	Unknown	454	U—Laptop	480
Disabled controls	275	Victim work area	300	M—Documents	240
Tampering	175	Personal vehicle	166	T—ATM	156
Skimmer	72	Victim public area	105	U—Desktop	152
Bypassed controls	62	Victim grounds	64	M—Flash drive	66
Surveillance	49	Partner facility	63	T—Gas terminal	53
Assault	29	Public facility	58	M—Disk drive	50
Snooping	7	Personal residence	53	Unknown	38
Unknown	6	Victim secure area	42	S—Unknown	37
Destruction	3	Partner vehicle	22	S—Database	27
Connection	3	Public vehicle	11	M—Unknown	20
Wiretapping	3	Other	7	M—Tapes	20
Other	1	Uncontrolled location	5	U—Unknown	18
Error					
Variety	#	Vector	#	Asset	
Misdelivery	845	Unknown	1158	M—Documents	1071
Loss	367	Carelessness	820	S—Web application	211
Publishing error	285	Inadequate processes	41	U—Desktop	132
Disposal error	277	Random error	11	S—Database	115
Misconfiguration	81	Inadequate technology	8	M—Flash drive	82
Unknown	45	Other	5	S—Mail	73
Gaffe	33	Inadequate personnel	3	M—Disk media	61
Other	33			Unknown	60
Malfunction	31			S—File	52

Table 2 (continued)

Error					
Variety	#	Vector	#	Asset	
Programming error	31			S—Unknown	51
Omission	22			U—Laptop	32
Classification error	4			M—Tapes	24
Data entry error	4			M—Disk drive	23
Malware					
Variety	#	Vector	#	Asset	#
Backdoor	229	Unknown	231	U—Desktop	281
C2	197	Email attachment	208	P—Unknown	217
Capture stored data	179	Direct install	64	S—Unknown	201
Downloader	176	Web drive-by	24	N—Router or switch	96
Unknown	146	Email link	9	U—Mobile phone	89
Spyware/Keylogger	141	Download by malware	5	S—Web application	82
Export data	116	Remote injection	4	Unknown	47
Scan network	106	Email autoexecute	4	S—Database	47
Exploit vuln	91	Other	3	U—POS terminal	39
Brute force	88	Removable media	2	P—End-user	29
Disable controls	76	Software update	2	P—System admin	22
Ransomware	67	Network propagation	1	U—Laptop	21
Other	64	Web download	1	S—POS controller	20
Social					
Variety	#	Vector	#	Asset	#
Phishing	302	Email	307	P—Unknown	301
Bribery	46	Unknown	63	U—Desktop	246
Pretexting	35	In-person	44	S—Unknown	182
Extortion	30	Phone	15	N—Router or switch	95
Forgery	16	Documents	13	U—Mobile phone	89
Unknown	15	SMS	12	P—End-user	73
Influence	11	Software	11	S—Database	63
Other	9	Website	5	S—Web application	54
Elicitation	2	Social media	3	P—System admin	25
Baiting	2	IM	1	Unknown	23
Propaganda	2	Removable media	1	S—Mail	22
Spam	1			M—Documents	21
Scam	1			P—Executive	21
Misuse					
Variety	#	Vector	#	Asset	
Privilege abuse	977	LAN access	895	S—Database	699
Possession abuse	194	Physical access	323	Unknown	190

Table 2 (continued)

Misuse					
Variety	#	Vector	#	Asset	
Data mishandling	157	Unknown	165	M—Documents	180
Knowledge abuse	150	Remote access	40	M—Payment card	71
Unapproved hardware	49	Non-corporate	28	S—Unknown	68
Unknown	46	Other	20	U—Desktop	56
Email misuse	23			S—Mail	46
Unapproved workaround	15			S—Web application	36
Net misuse	11			P—Unknown	36
Unapproved software	7			M—Unknown	25
Illicit content	5			P—End-user	24
Other	4			M—Flash drive	18
				U—Laptop	18

Environmental				Total	
Vector	#	Asset	#	Type	#
Unknown	3	S—Unknown	3	error	2038
Power failure	2	S—Web application	2	hacking	1927
Fire	1	N—Router or switch	2	misuse	1409
Humidity	1	S—Mail	1	physical	1343
		Unknown	1	malware	545
		S—Database	1	social	451
		S—File	1	unknown	224
		N—LAN	1	environmental	7

**Data as at 20 October 2017

legal and regulatory (226), response and recovery (172) and brand damage (136). These impact values cover the period 1972 to 2016.

An illustration of the results for impact rating is provided in Fig. 7. For most incidents, the true impact rating was not fully understood (599). There were 14 incidents rated as having a major impact, 31 incidents were rated as being moderate, 274 minor and 244 were rated as having no impact at all, i.e. null.

Victim demographics appear in Table 3. The most common country of victims was the USA (5121) followed by Great Britain (416), Canada (243) and Australia (96). Of all incidents, 169 were geographically unknown. Most victim organisations (990) had an employee count of over 100,000. Slightly less than this, 923 had an employee count of 1001 to 10,000. Those with 101 to 1000 employees sustained 700 incidents. Nine hundred thirty-eight victim organisations had between 1 and 100 employees. The majority of industries affected appeared to be in the public sector, with commercial bank (196) and Internet publishing (147) following marginally.

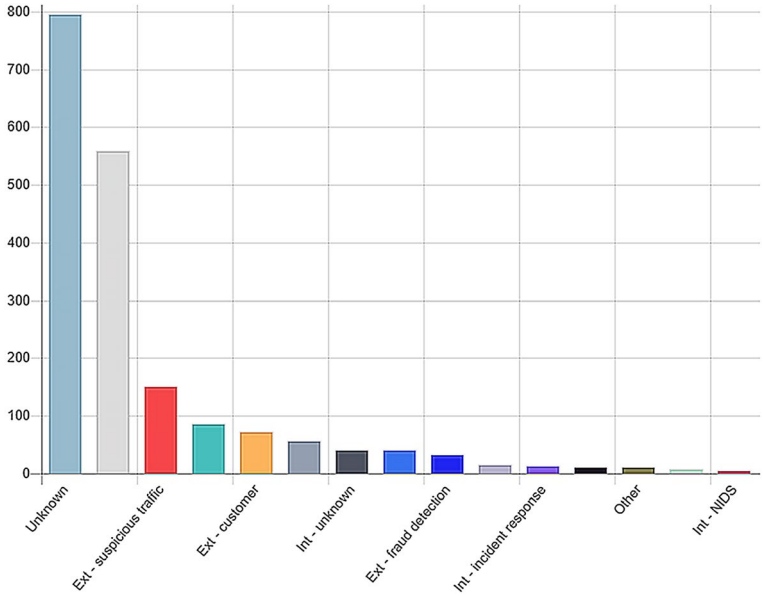

Fig. 3 A summary of the attack discovery method in the studied dataset

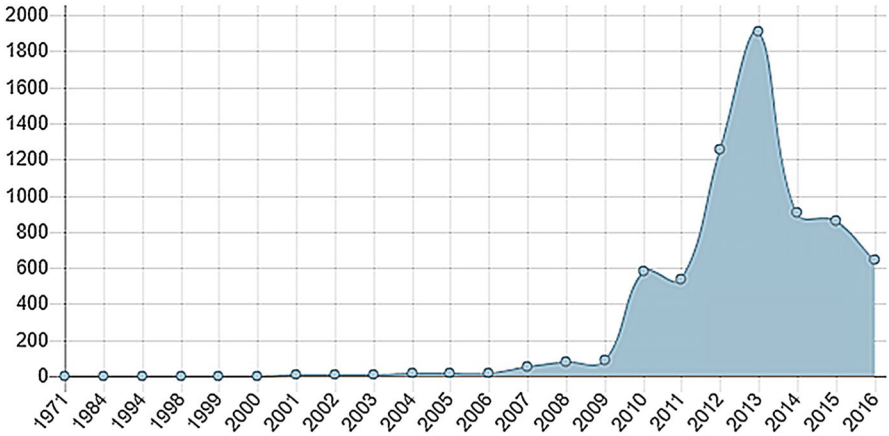

Fig. 4 The number of security incidents per year

6 Discussion

It is striking from an analysis of the dataset that despite the data being collected through the open-source community, it appears to represent the picture one might expect to see based upon the malicious trends industries are actively working to address.

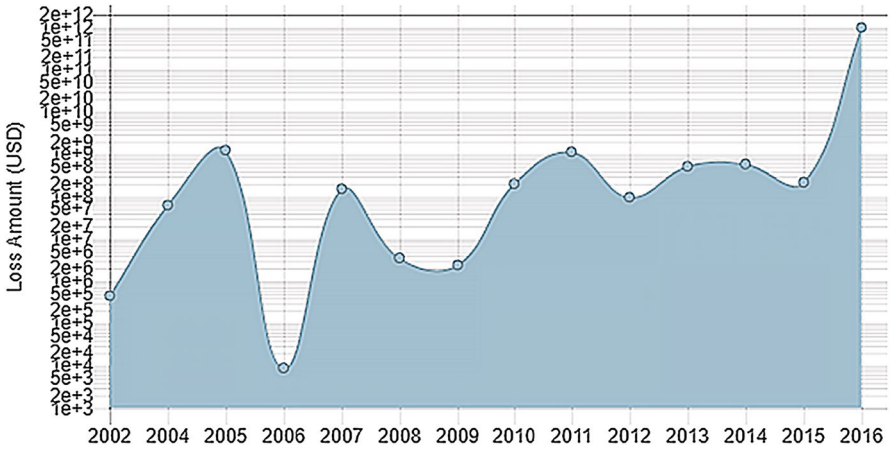

Fig. 5 The financial loss per year reported in the dataset

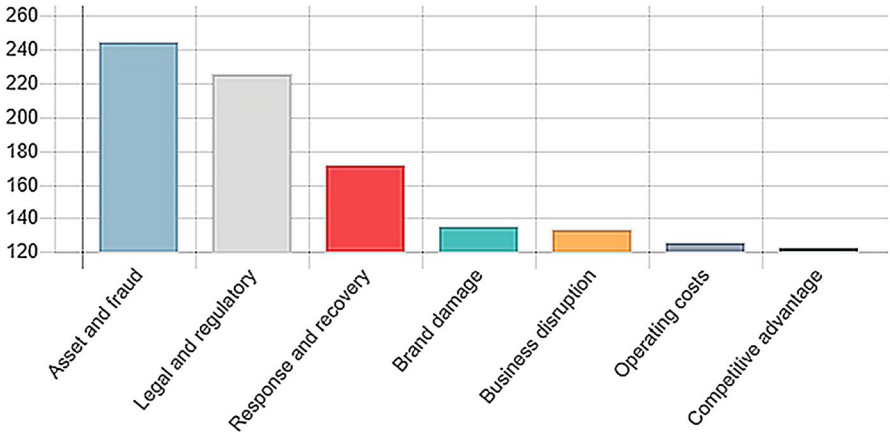

Fig. 6 The results pertaining to security incident impact variety

6.1 Frequency of internal attacks

The dataset shows that from 1972 to 2016, overall the number of internal actors and the number of external actors are roughly equal. This is important because computer systems are designed to mitigate threats from the outside inward, not usually the other way around [18]. The traditional view of computer security is that it should be organised like an onion with layers of security zones [8]. These configurations clearly have not mitigated the threats in this study as depicted in Fig. 3.

It is notable that the majority of internal attackers were end-users and system administrators, the two staff groups most trusted in a computing environment. Whilst the motivation in many attacks was not known, the majority of attacks were financially motivated. Another large proportion of attacks are noted as having been

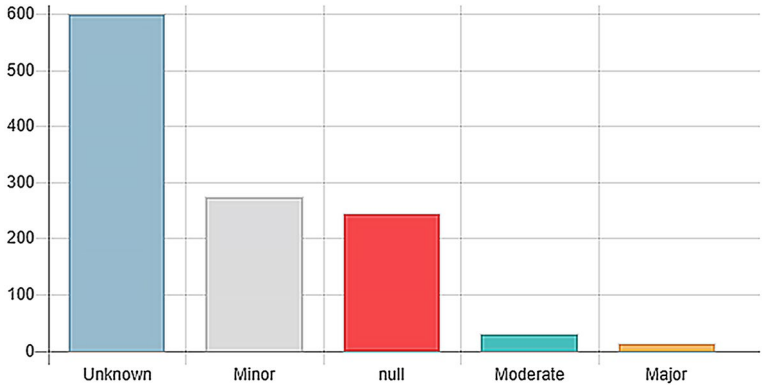

Fig. 7 An illustration of the results (summarised in Fig. 6) for impact rating

Table 3 Victim demographics data

Victims					
Country	#	Employee Count	#	Industry	#
US	5121	Unknown	2458	Administration of Veterans' Affairs	885
GB	416	Over 100,000	990	General medical and surgical hospitals	692
CA	243	1001 to 10,000	923	Offices of physicians (except mental health specialists)	334
Unknown	169	101 to 1000	700	Colleges, universities and professional schools	210
AU	96	11 to 100	558	Commercial Banking	196
NZ	73	1 to 10	380	N/A	187
IN	71	10,001 to 25,000	287	Internet publishing and broadcasting and web search portals	147
IE	48	Small	246	Administration of Public Health Programs	140
JP	44	Large	191	Direct health and medical insurance carriers	119
KR	41	25,001 to 50,000	160	Public administration	116
DE	40	50,001 to 100,000	101	Executive offices	116

** Data as at 20 October 2017

carried out for fun. Both of these findings are remarkable. These trends are likely a result of the increasing adoption and use of computer technologies to solve an increasing number of problems that were previously done offline. It appears that the increasing adoption of computers has led to a widened opportunity for attacks to take place.

6.2 Increasing rate and loss

It is apparent in Fig. 4 that cybersecurity incidents have dramatically increased since 2010. It is notable that this is approximately around the time of mass cloud

technology adoption and the general move towards Internet services [22]. The exponentially increasing incident rate from 2010 to 2013 is suggestive of a gauging exercise within computer security in which the dramatic change in the yearly rate of adoption of online services was too rapid for computer scientists and computer users to keep up technologically with what clearly appears to be a widened opportunity for malicious activity. Though the incident rate appears to drop, the amount of loss occurring per year is increasing exponentially. Figure 5 appears to represent a substantial sinusoidal pattern about 1e8 which appears to scale down towards 2e8 before the annual loss figure rapidly increases to 1e12.

6.3 Principle of least privilege

The statistical distributions in Table 2 are indicative of what can be expected based upon the state of the art, which is potentially suggestive of the accuracy of VCDB. The dataset tends to show that there is a direct relation between the mode of attack and the mode of use; in fact, they are the same in most cases. For example, in Table 2, malware and hacking have strong relations to backdoors left by system administrators. Misuse incidents frequently present as being a result of privilege abuse. Social incidents tend to be as a result of phishing. The most common error incidents involve misdelivery of confidential information. It is clear that in each case, the usage of a computer system is often its means of exploitation and destruction.

This closely ties with [24], which is the seminal piece of work in computer security that defined the principle of least privilege (POLP). The principle echoes the patterns that can be observed in Table 2. Given what can be observed, POLP is not enough in principle to secure a computer system. This is because, according to the dataset, even a design which follows POLP is still vulnerable because it can still be misused to some extent. The vulnerability lies in the ability of use, which POLP cannot address. Given that POLP is the most popular design pattern for a computer security configuration [25], this is a serious problem. Following this design pattern means that usability and access are a direct trade-off for security, which is a highly unsatisfactory position resulting in the shortcomings that can be observed, depending on where the balance falls during design.

6.4 The role of human error

The majority of attack modes relate to functional work and access arrangements for computer systems. The vectors for each attack mode show in clarity that these incidents are a result of bad practices, for example sending confidential information in a way that poses a risk of misdelivery. However, not all vectors appear to relate to user error but to the mode of use itself. All modes of attack appear to be an overall abuse of the privilege of being able to use the computer system, not any specific permission target. In these cases, it is not always possible to accurately determine fault because fault itself may be a philosophical question.

The recurring theme of data stores as an affected asset (documents and databases) seems to indicate that the object of cybersecurity incidents is information. This agrees with the well-known position that data is one of the most valuable assets in hi-tech economies. Thus, it can be properly concluded that if abuse of privilege is the means to procure those documents, then privilege itself is the incurable vulnerability. It is, in effect, a vulnerability which cannot be patched because by so doing, the computer system would be rendered unusable for the purpose intended. This begs the question of how and by what means security will not be a trade-off with functionality.

6.5 Criticality

The results for Tables 1 and 2 are organised in bands of criticality. This was spontaneous and not a result of placement. The most important criticalities are that in the majority of fields, important information was unknown. It is impossible to say with any degree of precision that this is for any specific reason, but it is likely that this is an indicator of successful repudiation. It is a concerning pattern that successful repudiation could feature significantly and suggests that current technology is unable to deal with the scale of malicious activity which organisations are facing.

Geographic criticalities are extremely important. The majority of victims seem to be located within western states, though this could be because information relating to other states is kept confidential. Those organisations on the extremes of size (the largest and smallest) in terms of employee count appear to be more vulnerable than others to cybersecurity incidents. This is likely to be because in a small organisation, it is probably financially less capable for the purposes of investment in cybersecurity and has less access to expertise than a larger organisation. In the largest organisations, it is likely to be very difficult to detect breaches and to mitigate a potentially higher rate of internal malicious activity. The scalability of computer security infrastructures is a known problem within the literature [10].

The most frequent assets targeted are documents, personal computers, databases and web applications. This is not surprising because each asset usually has to be compromised carefully in tandem in order to obtain the confidential documents. The attack methods tend to reflect the type of incident involved, in particular the public sector is affected the most by cybersecurity incidents followed by commercial banking, with both having greater criticality—this is probably because they are ideal targets given that the dominant motivations in the results seem to be financial and the asset targeted tends to be documents storing confidential information.

The majority of actors seem to come from the USA and Russia. Other strongly featuring geographic originators are countries with which there are known political and military conflicts, e.g. Syria, and so their presence among the results is not surprising. Most internal threats showed criticality in the end-user and financial motive, whereas external threats showed greater criticality in activism and nation state activity. This is consistent with what one might expect based on the state of global affairs.

The mode of attack and vectors tend to demonstrate a logical consistency with what is known about cyberattack patterns. For example, statistically phishing was

strongly associated with the vector of email. The vector in most attack modes was not known. Those vectors and attack modes showing greatest criticality were physical access, email and LAN access/backdoors. The attack modes showed greatest criticality in carelessness and privilege abuse—this ties in closely with established cybersecurity best practices and known modes of attack. This is concerning because the attack rates are still remarkably high even though there are well known mitigations against the same.

Moreover, this data adds to the perspective [2] that existing means of securing computer systems cannot 100% guarantee detection and mitigation of every threat. Though at first glance it may appear as though incident rates are decreasing, loss is increasing exponentially which challenges the very foundations of computer security. It suggests attackers are doing more damage through fewer activities and are thus becoming rapidly more capable.

7 Summary and conclusion

The objective of this research was to identify important trends amongst the largest publicly available dataset for cybersecurity. It also aimed to investigate the degree of randomness and the probability of extreme possibilities occurring in cybersecurity incidents; these incidents associated with the VCDB dataset because it is the largest cybersecurity incident dataset which is publicly available. This has been achieved with successful Monte Carlo simulation and by implementing a MapReduce function to take a sizeable JSON dataset and summarise it to respond to realtime queries from a web application. The general patterns identified from the MapReduce process were that there is a major increase in financial loss as a result of incidents, which are increasing in prevalence. It is becoming increasingly common for incidents to be internal in origin. It is becoming more popular for nation states to engage in acts of cyber warfare. In general, the trend appears to be that cybersecurity incidents are motivated either by ideology or financial motivation. It is to be expected that loss will continue to increase, prevalence will increase and the role of nation states in cyberattacks is likely to increase.

From the analysis in this study, it appears that the challenge faced by cybersecurity is on a theoretical battle ground. Present ways of thinking about cybersecurity trade usability with security. For instance, generalised access alone is a violation of Saltzer's principle of least privilege [24]. The balance between usability and security is, it is submitted, the source of the prevalence of modern cyberattacks. The field of computer security needs a fundamental way of providing access with a usable experience and implementation of the functional requirements intended, without any implication for security. In order to achieve that there needs to be a theoretical rethink of cybersecurity.

Multiple temporal datasets also need to be compared together with data which is more recent in order to understand the most recent security incident trends and the underlying social reasons for them as opposed to statistics in isolation. We provide a model from which this exercise can be executed repeatedly and reliably against the same and other datasets.

The types of attacks studied in this paper shows an increasing exploitation of vulnerabilities that are almost "extinct" in classical computing environments. This can be explained by the immature security mechanisms in Supervisory Control and Data Acquisition Systems (SCADA) networks which employs a number of purpose-built protocols such as DNP3, Modbus and BACnet. Often, the security protocols deployed in CPS are not corresponding with their criticality or they even they lack any security protection mechanism. Many of the potential attacks on CPS and IoT devices can be prevented using anomaly and/or intrusion detection systems; nonetheless, these are vulnerable to statistical induction as established in [30]. However, there is a need for tailored innovative security and management mechanisms at the device-level to enhance CPS resilience.

Detailed patterns of activity reflecting the motivations of attackers need to be explored in order to understand specific types of cyberattacks. Theory then needs to be shaped to those realities. A significant amount of future academic research needs to build further datasets tailored to specific modes of enquiry. Research is also required to develop new mechanisms for the prevention of cybersecurity incidents.

It is submitted that based upon the patterns observed in this research, there needs to be a greater understanding of how the stand-off between functional requirements and security can be addressed, particularly in CPS. It is apparent that functional requirements can and often do require a trade with security, and the relationship is directly proportionate. Yet in industry there is a very high motivation for features in pressured commercial environments where new features are required often to remain competitive. The pressure to release new features classically results in security being secondary. This is one area which requires further analysis and research.

"Zero trust" or trustless computing is also a key emerging paradigm which changes the approach taken to cybersecurity generally. However, it has so far been the child of commercial research organisations with little output from academia. Academically rigorous outputs in relation to zero trust are required so that it can be applied in situations where classical application of cybersecurity mitigations are impractical, such as in the case of IIoT where devices may not have enough computational power to encrypt data. Examples of such emerging research in academic includes [31].

References

1. Adebayo AO (2012) A foundation for breach data analysis. J Inf Eng Appl 2(4):17–23
2. Ashfaq AB, Ali MQ, Al-Shaer E, Khayam SA (2013) POSTER: revisiting anomaly detection system design philosophy. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, vol 13. ACM Press. https://doi.org/10.1145/2508859.2512529

3. Baker T, Asim M, MacDermott A, Iqbal F, Kamoun F, Shah B, Alfandi O, Hammoudeh M (2019) A secure fog-based platform for scada-based iot critical infrastructure. Softw Pract Exp. https://doi.org/10.1002/spe.2688
4. Barona R, Anita EM (2017) A survey on data breach challenges in cloud computing security: issues and threats. In: 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE, pp 1–8
5. Belguith S, Kaaniche N, Hammoudeh M (2019) Analysis of attribute-based cryptographic techniques and their application to protect cloud services. Trans Emerg Telecommun Technol. https://doi.org/10.1002/ett.3667
6. Böhme R (2016) Back to the roots: information sharing economics and what we can learn for security. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS'16. ACM, New York, NY, USA, pp 1–2. https://doi.org/10.1145/2994539.2994540
7. Bray T (2014) The JavaScript Object Notation (JSON) Data Interchange Format. https://doi.org/10.17487/rfc7159. Accessed 28 Oct 2017
8. Broderick S (2005) Firewalls—are they enough protection for current networks? Inf Secur Tech Rep 10(4):204–212. https://doi.org/10.1016/j.istr.2005.10.002
9. Carlin A, Hammoudeh M, Aldabbas O (2015) Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges. Int J Adv Comput Sci Appl 6(6):1–15
10. Chung Y (2012) Distributed denial of service is a scalability problem. ACM SIGCOMM Comput Commun Rev 42(1):69. https://doi.org/10.1145/2096149.2096160
11. Dean J, Ghemawat S (2008) Mapreduce: simplified data processing on large clusters. Commun ACM 51(1):107–113. https://doi.org/10.1145/1327452.1327492
12. Department for Culture, Media and Sport: Almost half of UK firms hit by cyber breach or attack in the past year - gov.uk (2017). https://www.gov.uk/government/news/almost-half-of-uk-firms-hit-by-cyber-breach-or-attack-in-the-past-year. Accessed on 26 Oct 2017
13. Durumeric Z, Kasten J, Adrian D, Halderman JA, Bailey M, Li F, Weaver N, Amann J, Beekman J, Payer M, Paxson V (2014) The matter of heartbleed. In: Proceedings of the 2014 Conference on Internet Measurement Conference, IMC'14. ACM, New York, NY, USA, pp 475–488. https://doi.org/10.1145/2663716.2663755
14. Elmellas J (2016) Knowledge is power: the evolution of threat intelligence. Comput Fraud Secur 2016(7):5–9
15. Gai K, Qiu M, Hassan H (2017) Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud computing. Concurr Comput Pract Exp 29(7):e3856. https://doi.org/10.1002/cpe.3856
16. Heinl C (2018) NTU Singapore cyber risk management project, key observations to enhance cyber resilience. Tech. rep., Department of Computer Science, Michigan State University
17. Ikpehai A, Adebisi B, Rabie KM, Anoh K, Ande RE, Hammoudeh M, Gacanin H, Mbanaso UM (2019) Low-power wide area network technologies for internet-of-things: a comparative review. IEEE Internet Things J 6(2):2225–2240. https://doi.org/10.1109/JIOT.2018.2883728
18. Juels A, Oprea A (2013) New approaches to security and availability for cloud data. Commun ACM 56(2):64–73. https://doi.org/10.1145/2408776.2408793
19. Luiijf E, Klaver M (2015) On the sharing of cyber security information. In: International Conference on Critical Infrastructure Protection. Springer, pp 29–46
20. Mackintosh M, Epiphaniou G, Al-Khateeb H, Burnham K, Pillai P, Hammoudeh M (2019) Preliminaries of orthogonal layered defence using functional and assurance controls in industrial control systems. J Sens Actuator Netw 8(1):14
21. McKinnel DR, Dargahi T, Dehghantanha A, Choo KKR (2019) A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. Comput Electr Eng 75:175–188. https://doi.org/10.1016/j.compeleceng.2019.02.022
22. Pinheiro P, Aparicio M, Costa C (2014) Adoption of cloud computing systems. In: Proceedings of the International Conference on Information Systems and Design of Communication, ISDOC'14. ACM, New York, NY, USA, pp. 127–131. https://doi.org/10.1145/2618168.2618188
23. Saleem J, Hammoudeh M, Raza U, Adebisi B, Ande R (2018) Iot standardisation: Challenges, perspectives and solution. In: Proceedings of the 2Nd International Conference on Future Networks and Distributed Systems, ICFNDS'18. ACM, New York, NY, USA, pp. 1:1–1:9. https://doi.org/10.1145/3231053.3231103

24. Saltzer JH (1974) Protection and the control of information sharing in multics. Commun ACM 17(7):388–402. https://doi.org/10.1145/361011.361067
25. Schneider F (2003) Least privilege and more. IEEE Secur Priv Mag 1(5):55–59. https://doi.org/10.1109/msecp.2003.1236236
26. Verizon RISK: vz-risk/vcdb: Veris community database (2017). https://github.com/vz-risk/VCDB. Accessed 26 Oct 2017
27. Walker-Roberts S (2017) Jsdoc: Home. https://steven.walkerroberts.co.uk/verisdb-analyst/. Accessed 26 Oct 2017
28. Walker-Roberts S (2017) Veris json data not compliant with json spec. issue #10292 vz-risk/vcdb . https://github.com/vz-risk/VCDB/issues/10292#issuecomment-340160543. Accessed 30 Oct 2017
29. Walker-Roberts S (2017) walkerandco/verisdb-analyst: an application for realtime visual and interactive analysis of verisdb incident data. the server uses isomorphic javascript and mongodb to analyse the data at lightning fast speeds. https://github.com/walkerandco/verisdb-analyst. Accessed 26 Oct 2017
30. Walker-Roberts S, Hammoudeh M (2018) Artificial intelligence agents as mediators of trustless security systems and distributed computing applications. Springer, Cham, pp 131–155. https://doi.org/10.1007/978-3-319-92624-7_6
31. Walker-Roberts S, Hammoudeh M, Dehghantanha A (2018) A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. IEEE Access 6:25167–25177
32. Walshe M, Epiphaniou G, Al-Khateeb H, Hammoudeh M, Katos V, Dehghantanha A (2019) Non-interactive zero knowledge proofs for the authentication of iot devices in reduced connectivity environments. Ad Hoc Netw 95:101988. https://doi.org/10.1016/j.adhoc.2019.101988