Multidisciplinary International Journal of Research and Development

Volume: 01 | Issue: 02 | 2021 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Subsisting Cyber Security Concerns and Possible Future Trends

Nzadon David[1], and Opani Aweh[2]

[1,2]Department of Mathematical and Physical Sciences (Computer Science Programme) College of Sciences Afe Babalola University. Ado-Ekiti, Ekiti State, Nigeria.

Email: [1]tufenzadon@gmail.com

Abstract— The deep space and the stunning level of sophistication of cyberattacks on critical infrastructures, facilities and services on which our contemporary existence has become increasingly dependent, is cause for great concern. Even though a great deal goes unreported, the reports available so far is alarming. What this implies is that we are existing at the precipice of a cyber-holocaust, it appears that the threats posed by these occurrences are not properly understood by the relevant stakeholders and the society in general. In this study, confirmed occurrences of successful cyber-attacks are presented in an extensive literature review. And based on this review pertinent data from secondary sources that have a keen interest in ensuring a secure cyber space is used to highlight subsisting and persisting threats. The information is also used to show future threats as regards the security of cyber space as the world anticipates intensification of cyber-attacks especially among state actors, as well as sophisticated corporate syndicates and highly motivated knowledgeable groups and individuals. From the analysis it appears that the approaches currently put in place to check/mitigate the incidence of cyber-attacks are not producing veritable results. Consequently, this study suggests the need to develop frameworks that will support multi and trans disciplinary approaches to the problem as well as improve/ enhance treaties among nations and the need for nations and corporate institutions and to take responsibility for cyber escalation.

Keywords— Cyberspace, cybersecurity, critical infrastructure, cybercrime, transdisciplinary cyber-frameworks, threat actors.

I. INTRODUCTION

We are becoming increasingly dependent on technology, and this increased dependency is fuelled by the convenience provided by information technology which has automatically given rise to an alternative space (cyber space). We are now living in a dual space system which consists of the physical space as well as the cyber space, going by the blitzing pace of technology and innovation, we are tilted more towards cyber space than the physical space, for example governments, corporate institutions, individuals and some entire components of some cities interact more with cyber space than with the physical space that used to be the norm. Technologies like Internet of Things (IOT) have introduced another dimension to how we use cyberspace. With this increasing dependency and mushrooming threats, most of which go unreported the world is on a delicate balance that requires in depth study and analysis to guarantee future survival. It is already established that the war between states now and in future are and will be cyber based, there are well established institutions across the globe whose major preoccupation is cyber-attacks on governments, corporate institutions and individuals, Again most individuals and groups thrive off cyber space through acts that are inimical to the future of society as regards cyber space: these are those whose perpetrate one criminal act or the other for malice or financial gain, in fact many individuals and groups live off this criminal act, and their population is on the rise. The ease and convenience by which violations in cyberspace are perpetrated and the huge gains to the perpetrators is an enormous motivation for the escalation of these attack and other threats. Amidst these attacks as well and its sundry devastating side effects which often results in monumental losses (financial and otherwise) the world is undeterred as it forges towards everyone become digital natives.

In this study, a cursory look at the subsisting and persisting cyber threats and cyber related incidences are evaluated to show some of the trends that can be to used to forecast or predict what the future might hold for the cyber space and to advance recommendations to mitigate against threats and attacks. We need to be properly informed and guided an in our transition to becoming consummate digital natives. To accomplish this, data gathering from secondary sources was employed and used to piece together reliable information provided by distinguished institutions and firms that are committed to providing secure interactions in cyberspace and guaranteed survival of cyberspace.

II. LITERATURE REVIEW

In a world driven more and more by big data, social networks and online transactions, information stored or managed via the internet and automated processes performed through the use of IT systems, information security and data privacy are permanently facing risks [17]. Critical Infrastructure Systems (CISs) which include sectors such as finance, transportation, oil, energy and water distribution, emergency services, health and government. These systems from the point of view of security are of increasing importance in both industrial and public domains [49]. They have to be highly resilient against cyber attacks and malicious activities, in order to reduce the risk of severe failures, as well as compromise of sensitive data. The criticality of such systems poses new challenges for computing professionals, which must develop more robust systems to ensure a high level of protection, and at the same time they must keep low costs and development time [18]. The scope of Cyber-attacks and threats keeps on stretching by the day: In October 2012, NATO identified an extensive espionage attack which was accredited to Russia and was going on for five years. This attack targeted European and Ukrainian government institutions [72]. Also in 2020, Iranian General and leader of the Quds group Qassem Suleimani was reported to have been killed by the Multi-Spectral Targeting System MQ-9 Reaper Drone [78]. Large retailers have also been targeted. this includes Target in December of 2013 [129] and Home Depot in mid-2014 [70].

The health sector also hasn’t been exempted from attacks as evidenced by the Anthem Health Insurance Breach [120]. Furthermore, in 2018 Singapore’s experienced its worst ever cyber-attack, when hackers got access to SingHealth’s system and stole the personal particulars of 1.5 million patients including Prime

Minister Lee Hsien Loong and a few other ministers [132]. This is in addition to the devastating "ransomware" called WannaCry that crippled computers in hospitals across the UK and cost the NHS £92m [50].

The Aviation industry has also seen its fair share of attacks over the years. In 2006, July a cyber attack forced the American Federal Aviation Administration to shut down several Air Traffic Control systems in Alaska [43] [86]. Equivalently, in August 2008 at Spain's Madrid-Bajaras airport, a trojan in one of Span Air's main computer systems blocks the reception and activation of an alarm message from flight No. 5022. This was cited among the causes of the plane's collision and the loss of 154 passenger lives [38]. It has yet to be determined whether the systems were intentionally compromised through the Trojan [57]. Also, in March 2014 Malaysia Airlines flight MH370 disappears from tracking radar, and the Boeing 777-200ER is later given up for lost in an airline press release. In the overall uncertainty surrounding the event, it was also suggested that the plane had been commandeered by means of a mobile phone and/or a USB drive [38]. The theory has never been proven and has been roundly rejected by Boeing [155].

Cyber criminals have also targeted Government establishments numerous times over last few decades. In December 2015, in Ukraine, a cyber-attack was identified on multiple electricity distribution centres which caused power outages and affected approximately 225,000 customers [109]. Other attacks were carried out on call centres to stop customers to contact power the company and get help [72]. Also, in 2017 the city of Atlanta suffered an attack that locked down the city systems for over a week [19]. Similarly, a "logic bomb" was reportedly inserted in the Trans-Siberian pipeline's control software to abnormally change the pumps and valves settings, causing a massive explosion in 1982 [108]. Perhaps the most famous cyber-attack on a government establishment was the "Stuxnet" virus between late 2009 and early 2010. This virus was allegedly responsible for destroying about 1,000 Iranian high-speed centrifuges used for Uranium enrichment, through periodically changing the rotational speed of the centrifuges, significantly shortening their lifespans [7].

The Hospitalities and Leisure Industry are also not immune to cyber-attacks. Not even the world's largest hotel company could protect itself from cyber disaster [134]. In September 2018, Marriott hotels announced it had suffered a massive data breach affecting nearly 400 million customers to theft [113]. The breach started in 2014 and unfolded over years with attackers stealing contact information, passport numbers, arrival and departure dates, and reservation information. This breach represents one of the largest in history.

Universities have also fallen victim to state-sponsored cyber-attacks. In March 2018, the U.S. government charged nine Iranians with stealing data and intellectual property from 300 domestic and foreign universities over a three-year period [40]. Reports estimate more than 31 terabytes of information worth more than $3 billion worth of intellectual property. "Spear-phishing" was used by the attackers to obtain login information of university. More than 100,000 professors were targeted while 8,000 accounts were successfully infiltrated—almost half of which were accounts at U.S. schools. The alleged culprits are still believed to be in Iran.

Another salient but important cyber threat issue, is that of privacy. While appearing minor in view of other cyber risks, privacy and personal data breaches heavily impact both consumers and organisations [56]. For instance, the average financial loss due to the theft of a single piece of private data is estimated to be 213 USD [61] [149]. Cambridge Analytica came into the limelight for the first time in 2015. Ted Cruz utilized the company during his campaign. The world will later on learn about the use of personal data for Facebook users [37]. According to different media sources, Strategic Communications Laboratories, which is the parent company of Cambridge Analytica, was working with Global Science Research (GSR) [145]. GSR founder Kogan A. who at the time was head of data collection processes. He used Amazon Mechanical Turk, or MTurk, through which the users were presented with an opportunity to do routine and minimum paid job – Kogan offered the users to do online survey in exchange for the payment of 1-2$ [21]. In order to complete the survey, the users were asked to connect their Facebook accounts to the website [21]. This automatically led to unintentionally connecting Facebook "friends" of a user – the information of these "friends" became available for data collectors as well [151. This "seeding" technique proved to be very effective [145]. It was possible to get information about a huge number of people through one user. On average a single user brought around 340 "friends" according to the information based on 2014 statistics.

User Information such as location and interest were gathered and analysed with the five-factor model – dispositional model of personality [61]. The analysis could unravel such traits of a person as extraversion, benevolence, conscientiousness, emotional stability and openness to experience, as well as their opposites [145]. Amazon has blocked GSR access to MTurk after numerous complaints [21].

Despite the increase in cybersecurity spending year after year by both the public-sector and private-sector, the number of cybercrime incidences keeps rising, and the growth of cybercrime appears no closer to being contained [145]. There are several challenges to countering cybercrimes: [11] law enforcers internationally are overwhelmed by the rampant spread of cybercrime and the rapid growth of dark web and underground cybercrime platforms. There is also the prevailing climate of a lack of efficient information sharing of cyber incidents between organizations due to non-disclosures, anti-trust or privacy laws. This has severely hampered the coordination levels observed among law enforcements across the borders [18]. Firms in the private sector are spending money almost exclusively in defending their own "four walls", which does not address directly the external actors of cybercrimes [145]. Also, firms in many Asian countries choose to underinvest in cybersecurity due to partial externalization of data breach costs, and the absence of legal liability to protect vulnerable third parties who entrust their digital assets to firms for processing [145]. There is also a need for an integrated approach between private sector involvement and business solutions in order to counter cyber threats [52].

No sector or industry is immune to cyber-attacks and while it is rare to find cyber-attacks that are similar it is imperative to understand the types of attacks, trends of attacks, the most targeted sectors, regions with the most persistent offenders as well as the type of defense/response utilized against various cyber threats. Multiple studies and surveys focus on specific cybercrime characteristics or develop classification models that do not adequately address the complexity of this contemporary type of crime [135]. An exploratory analysis is therefore imperative in order to come up with trends that could be insightful for individuals, corporations, and countries to measure not only the damages caused by cyber breaches, but also to provide a foundation for future comparisons one that can serve as a basis for proactive measures within industry and organizations.

Related Studies

[121] in their study titled "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments" introduced a cybersecurity framework that identifies the malicious edge devices in the distributed fog computing environment through the two-stage Markov model namely Markov1 which is the first stage Markov model which calculates the attack probability of the edge device and its category. Markov2 is the second stage Markov model which predicts whether the edge device should be shifted to Virtual Honey Pot Device (VHD) or not on the basis of information sent by Markov1, the framework has been tested with real attacks in virtual environment (through Open stack and Microsoft Azure). The experimental results indicate that the framework is successful in identifying but is restrained to preventing attacks from malicious edge device [121].

[135] introduced a comprehensive framework that sought to tackle cybercrime incidents. The framework involves an assesment of the severity of the attack threat which was done by a combination of frequency of: (i) appearance/reference and (ii) number of incidents. The framework also includes a detailed and relevant action plan for the relevant stakeholders involved in dealing with cybercrime. The study resulted in the creation of a comparison table of the top 15 cyber-threats and their trends. Each trend derives from the comparison of threat frequencies [135].

[31] presented a theory of insider threat assessment. They utilized a modelling methodology to capture several aspects of insider threat, and subsequently, show threat assessment methodologies to reveal possible attack strategies of an insider. The model was tested against a couple of common insider threat scenarios.

[128] in their study developed a novel multi-layer cloud architectural model is to enable effective and seamless interactions/interoperations on heterogeneous devices/services provided by different vendors in IoT-based smart home. They also tried to solve the heterogeneity issues in the presented layered cloud platform, an ontology-based security service framework is designed for supporting security and privacy preservation in the process of interactions/interoperations.

[88] in their study sought to enhance the use of CVSS for vulnerability scoring, they utilized game theory to modelling an attacker-defender scenario and argue that, under the assumption of rational behaviour of the players, an effective vulnerability patching strategy could be achieved with an optimal strategy, solving the game. Their strategies were implemented as new functionality in the software tool CAESAIR. This research builds on our previous studies, where CVSS was used to inform the design of the utility functions, by performing the Nash equilibrium analysis of the game.

III. DATA CLASSIFICATION AND DATA ANALYSIS

Average Size of a Data Breach

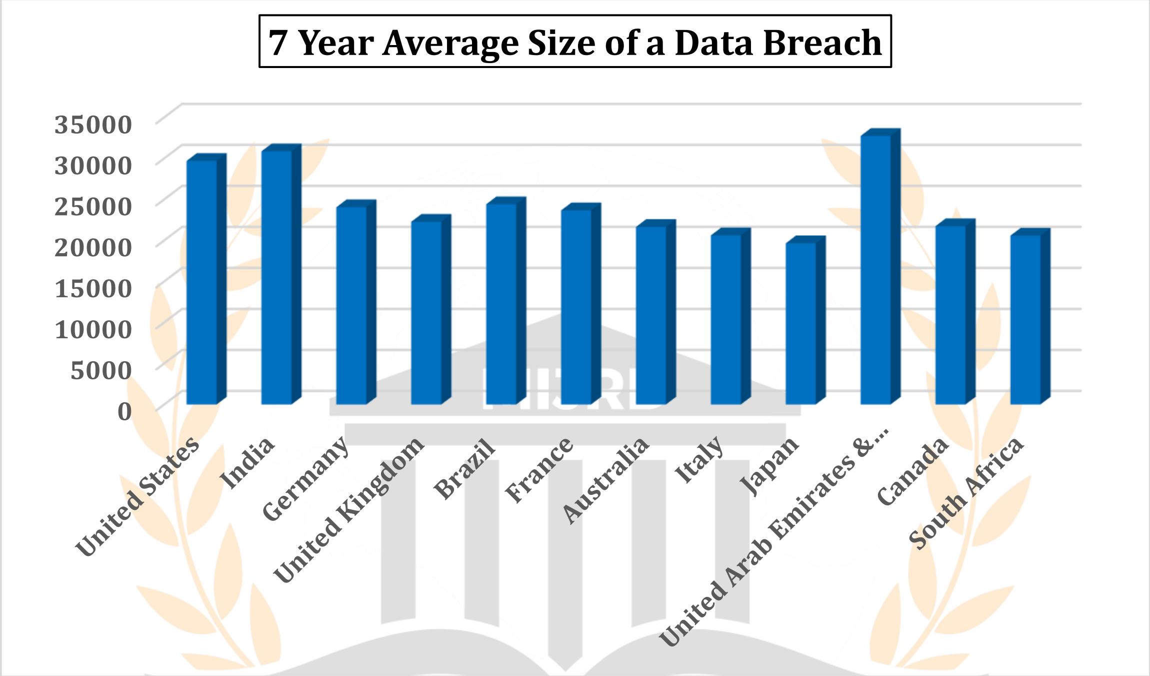

Figure 1: 7 Year Average Size of a Data Breach

The average size of a Data Breach looks at the average number of total records per country/Region that have been compromised during a breach. The UAE & Dubai is out in front with a 5-year average of 32741 breaches. The region has also seen a yearly increase in the number of breaches.

India and also follow closely behind with a total 7-year average of 30873 breaches. India has also seen a consistent rise in the average number of yearly breaches. the United States make up the top three with a 7-year average of 29706 breaches despite having a decrease in 2015 and 2017, Brazil and France make up the remaining top 5 with France also experiencing a consistent yearly increase except for the year 2015.

The bottom 5 countries/ regions are made up of Japan, South Africa, Italy, Australia and Canada with Japan having the lowest 7-year average of 19661 records despite having seen a yearly increase in all but 2018. South Africa and Canada also make the bottom 5 despite having a experienced a consistent yearly increase, although the average for those countries is 4 and 5 years respectively.

The top 5 countries/regions combine for an estimated population of 2 billion people while the bottom countries /region combine for an estimated 311 million people. This shows that in spite of advanced technology and sophistication, the sheer number of people corelates with the number of data breach attempts.

Average Yearly Cost of a Data Breach

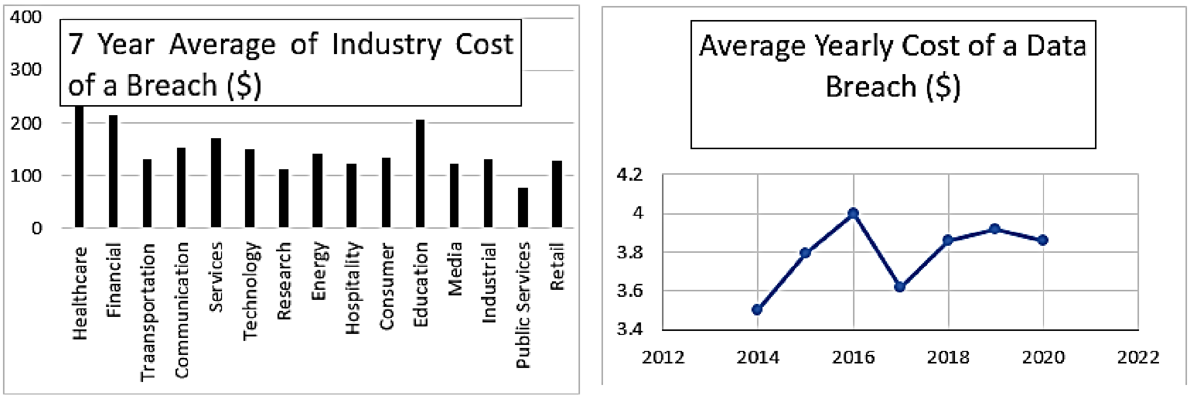

Figure 2 & 3: 7 Showing 7-year average industry cost of a data breach and average yearly cost of a data breach respectively

The average yearly cost of a data breach shows the total average 7-year cost of a data breach from 12 countries/regions. This total average peaked at an all-time high of 4$ in 2016.

Average Industry Cost of a Data Breach

The average industry cost of a data breach looks at the industries that have been most affected in terms of the average cost of a data breach. The healthcare which consists of hospitals and clinics sector surprisingly leads the line with a 7-year average cost of 361 $, the healthcare sector has also seen a yearly increase for all but one year (2016) of the stipulated time frame. the finance industry which consists of Banking, insurance and investment companies unsurprisingly came in at second with a 7-year average cost of 217$. Furthermore, the sector has also experienced a year-on-year increase for all but one of the stipulated time frame. The educational sector which consists of Public and private universities and colleges, training and development companies is third with a 7-year average cost of 209 $. The services industry which consists of (Professional services such as legal, accounting and consulting firms) and the communication sector which consists of Newspapers, book publishers, public relations and advertising agencies make up the top 5. The industry with the least average cost of a breach is the public services industry which consists of the Federal, state and local government agenciesas well as NGOs with a 7-year average of 79$. The other industries that make up the bottom five includes industries such as the Research Industry (brick and mortar and e-commerce), the hospitality industry (hotels, restaurant chains, cruise lines), the media industry (Television, satellite, social media, Internet) and the transportation industry (Airlines, railroad, trucking and delivery companies). It can be seen that the heavily regulated industries such as healthcare, financial and communications had a average data breach cost that is substantially higher than the less regulated industries such as retailers and the public sector industry.

Detection and Escalation Cost

These are costs associated with detection and escalation of data breach incidents. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors.

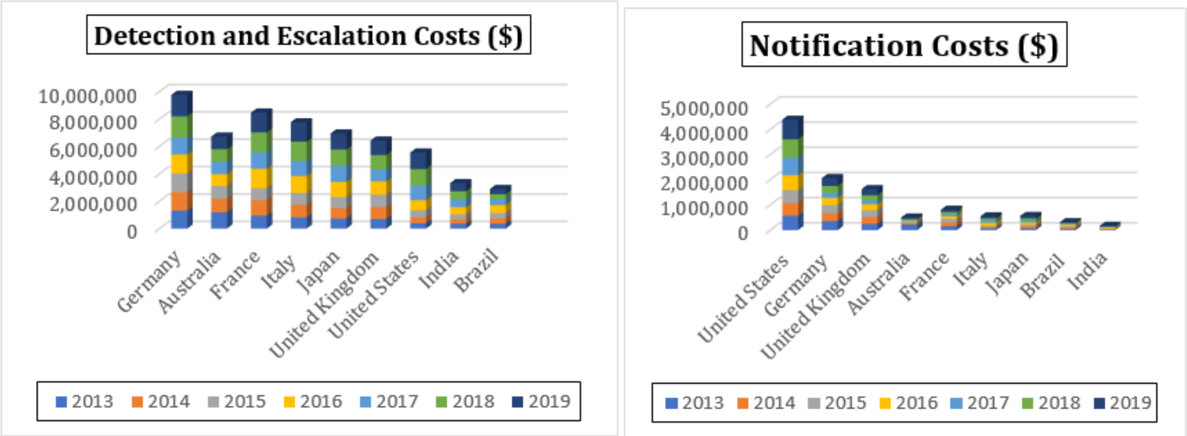

Figure 3 & 4: Showing Detection and notification cost respectively

Germany is out in front when it comes to detection and escalation cost with a 7-year average detection and escalation cost of 1,396,312. Unsurprisingly Germany also saw an increase in detection and escalation cost for 5 out of the 7-year period. France is next on the list with a 7-year average of 1,210,871. France also unsurprisingly saw an increase in detection and escalation cost for 4 out of the 7-year period. Italy, Japan and Australia complete the top 5 with a 7-year average of 1,109,696, 992,418 and 960,051 respectively. Brazil has the least detection and escalation cost out of the designated countries/regions with a 7-year average of 412,999 Surprisingly, Brazil saw an increase in detection and escalation cost for 4 out of the 7-year period. They are closely followed by India with a 7-year average of 475,521. India has also seen an increase in 5 in out of the 7-year period. The United States completes the bottom 3.

Notification Cost

These are all the costs associated with notification activities in the event of a data breach. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. The US sample experienced the highest notification cost. The United States is out in front when it comes to detection and escalation cost with a 7-year average of 625,499. Unsurprisingly, the United States has seen an increase in notification cost for 5 out of the 7-year period. Germany is next on the list with a 7-year average of 294,885. Germany also unsurprisingly saw an increase in notification costs for 4 out of the 7-year period. The United Kingdom, France and Japan complete the top 5 with a 7-year notification average of 231,626, 115,431 and 80,170 respectively. India has the least notification cost out of the designated countries/regions with a 7-year average of 23,702. Surprisingly, Brazil has seen an increase in notification cost for 3 out of the 7-year period. They are closely followed by Brazil with a 7-year average of 44,658. Australia completes the bottom 3.

IV. FUTURE TRENDS

Evolution of Cybercrime/Cybercriminals

In the coming decade cybercriminals will modify, adapt, and diversify their attack strategies states, this is will happen despite the increased actions of law enforcement actions against cybercriminals and crime syndicates in the past decade, Furthermore, an increased maturity and resilience among threat actors will ensure that they remain operational despite the clampdown by various law enforcement and agencies. A closer exploration also indicates that conventional cybercrime and financially-motivated, targeted attacks will continue to pose a significant threat to corporations, businesses as well as individual users and. However, criminal operations will likely continue to alter their techniques in order to reduce the risk of exposure, detection and disruptions. Cybercriminals will also seek to capitalize and streamline their efforts in several ways such as: moving away from partnerships to operating within close-knit syndicates; leveraging on the familiarity and exposure with local environments; using third parties to sell and buy direct access to networks for ransomware attacks instead of carrying out advanced intrusions, increasing the accuracy of targeting by using valid documents to prime out possible victims before attacking.

Rising Vulnerability of Cloud Infrastructure

The middle east/Africa sub region has seen a 42% rise in exabytes of cloud data within the study period. Africa's shortcomings in wired infrastructure has made the region a good place for cloud adoption [64]. One of the key results of the lack of decent and affordable wired services is that people have instead adopted mobile application services [64]. In some cases, mobile applications of certain types have usage statistics that dwarf even the US's [152]. An example is Safaricom's M-PESA mobile payment system, which provides a way for customers to transfer money to each other through mobile phones [152]. Compared to wired infrastructure, the deployment of mobile bandwidth in Africa is significantly easier, both from a financial and cultural perspective [152]. A recent World Bank study even revealed that 97 percent of Africa's population can be covered by mobile without the need for any government subsidy [152]. Furthermore, the discovery of multiple side-channel vulnerabilities in modern CPUs over the last two years could pose a high risk to organizations running their compute infrastructure in the public cloud [115]. Adversaries can use this class of side-channel vulnerabilities to read sensitive data from other hosts on the same physical server [115].

Rise in Geopolitical Tensions

The very beginning of 2020 was marked by a sudden increase in tensions between Iran and the U.S., including military action undertaken on both sides [36]. Although rhetoric de-escalated by mid-January, hacktivism, disinformation campaigns on social media, as well as an elevated risk of targeted intrusions (including destructive attacks) will go into the future [36]. Global businesses may find themselves in the crosshairs as geopolitical tensions persist [5]. As cyberthreat actors take advantage of high-profile global events and seek to influence mass opinion, we can expect these actors to not only sustain current levels of activity but also to take advantage of new capabilities as new technologies enable more-sophisticated threat TTPs [5].

Rise of the Insiders

Over the years a lot of attention and resources have been devoted to malicious/criminal attack and with good reason as well, as this category of attack has seen a year-on-year increase for all but one year during the 7-year period. However, the combined categories of system glitches and human errors do in fact account for a higher cause of breaches over a 7-year period. This indicates that as much as attacks from external actors shouldn't be neglected, a lot of damage can be done from internal actors either inadvertently or otherwise. This is a trend that will undoubtedly persist into the next decade unless novel strategies can be deployed to combat them.

The Healthcare Frontier

The healthcare which consists of hospitals and clinics sector has consistently ranked high in tserms of the data breach cost. The industry has 7-year average data breach cost of 361 $, the healthcare sector has also seen a yearly increase for all but one year (2016) of the stipulated time frame. With the scramble to develop and distribute vaccines in a post pandemic world. This industry will continue to be among the hardest hit.

V. CONCLUSION

When Robert Metcalfe made his popular prediction that sought to explain how networks will spread in in the future, it was deemed audacious. In what is popularly referred to as the Metcalfe law which states that the value of a network is directly proportional to the to the square of is number of users [116], it was considered ludicrous. That prediction has now been surpassed as networks have become invaluable and totally indispensable. Modern day existence is now principally hinged on networks, a substantial part of daily transactions worldwide is conducted and supported by computer networks.

Networks are an integral part of the business, social, economic and political aspects of states, corporate entities, individuals etc. The Cybersecurity and Infrastructure Agency of the USA, identified 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States and the world thereof that their incapacitation or destruction would have a debilitating effect on security, economy, national public health or safety, or any combination thereof. These Critical Infrastructure Systems (CISs) which involve sectors such as energy, finance, food and agriculture transportation, healthcare, public health, oil, gas, water distribution, government and emergency services have all become almost completely reliant on computer networks [49]. As nations target other nations infrastructure, and as competitors target each other's corporate information and as hackers intensify their criminal and malicious attacks. A paradigm shifts in addressing and mitigating possible cyber-attacks has become germane.

Consequently, this study advocates and supports the call for the development of a multidisciplinary, and transdisciplinary based strategies to contain the threats that have persisted and have seemingly defied existing solutions. Studies that can help to develop veritable, multidisciplinary, transdisciplinary frameworks upon which future strategies will depend have become imperative. also, treaties, effective legislation, appropriate sanctions and the need for nations, corporate institutions, and individuals to be take responsibility as well as be held accountable have become indispensable.

REFERENCES

[1] 9126-1:2001, I. (2001). Software Engineering – Product Quality – Part 1: Quality Model. International Organization of Standardization (ISO).

[2] Abedin, M., Nessa, N., Al-Shaer, E., & Khan, L. (October 2006). Vulnerability analysis For evaluating quality of protection of security policies. Proceedings of the 2nd ACM Workshop on Quality of Protection (QoP) (pp. 49 - 51). Virginia, USA: ACM. doi:10.1145/1179494.1179505

[3] Abraham, S. (2014). Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains. Journal of Communications, 899 - 907. doi:10.12720/jcm.9.12.899-907

[4] Abraham, S., & Nair, S. (2015). Exploitability analysis using predictive cybersecurity framework. IEEE 2nd International Conference on Cybernetics (CYBCONF) (pp. 317 - 323). Gdynia, Poland: IEEE. doi:10.1109/CYBConf.2015.7175953

[5] Accenture. (2019). Cyber ThreatScape Report .

[6] Akdeniz, Y., & Ellison, L. (1998). Cyber-stalking: The regulation of harassment on the ınternet (Special Edition: Crime, Criminal Justice and the Internet). Criminal Law Review. Retrieved December 04, 2020, from http://www.cyber-rights.org/documents/stalking

[7] Albright, D., Brannan, P., & Walrond, C. (2011). Stuxnet malware and Natanz: Update of ISIS December 22, 2010 report. Institute for Science and International Security, 15, 739883 - 3.

[8] Ali, A., Zavarsky, P., Lindskog, D., & Ruhl, R. (2011). A Software Application to Analyze Effects of Temporal and Environmental Metrics on Overall CVSS v2 Score. 2011 World Congress on Internet Security (WorldCIS-2011) (pp. 109 - 113). London, UK: IEEE. doi:10.1109/WorldCIS17046.2011.5749893.

[9] Al-Khateeb, H. M., & Epiphaniou, G. (2016). How technology can mitigate and counteract cyberstalking and online grooming. Computer Fraud & Security, 17(1), 14 - 18. doi:10.1016/s1361-3723(16)30008-2

[10] Anderson , R., & Moore, T. (2006). The Economics of Information Security. Science, 314(5799), 610 - 613. doi:10.1126/science.1130992

[11] Angwin, J., & Stecklow, S. (2010, October 12). Scrapers' Dig Deep for Data on Web. Retrieved December 06, 2020, from https://www.wsj.com/articles/SB10001424052748703358504575544381288117888

[12] AT&T. (2015). What Every CEO needs to know about Cybersceurity: Decoding the Adversary AT&T Cybersecurity Insights Volume 1. Texas, USA.

[13] AT&T. (2016). The CEO's Guide to Securing the Internet of Things: Cybersecurity Insights Volume 2. Texas USA.

[14] Ball, R., & Fink, G. A. (2004). Home-centric visualization of network traffic for security administration. Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security (pp. 55 - 64). Washington, USA: ACM.

[15] Bass, T. (2000). Intrusion Detection Systems and MultiSensor Data Fusion. ACM, 99 - 105. doi:10.1145/332051.332079

[16] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. 7th International Conference on Financial Criminology (pp. 24 - 31). Ocxford, United Kingdom: Elsevier Procedia. doi:https://doi.org/10.1016/S2212-5671(15)01077-1

[17] Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance Issues and Practice 40 (1),, 40(1), 131 - 158.

[18] Blinder, A., & Perlroth, N. (2018, March 27). A Cyberattack Hobbles Atlanta, and Security Experts Shudder. Retrieved from Nytimes.com: https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

[19] Board, E. C. (1998, January 01). Legal Aspects of Computer-Related Crime in the Information Society. Wurzburg, Germany. Retrieved December 02, 2020, from https://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html

[20] Boldyreva, E. L., Grishina,, N. Y., & Duisembina, Y. (2018). Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. European Proceedings of Social and Behavioural Sciences EpSBS. St Petersburg, Russia: Future Academy. doi:10.15405/epsbs.2018.12.02.10

[21] Boutang, Y. M. (2011). Cognitive Capitalism. Cambridge, UK, UK: Polity Press. doi:10.1111/1478-9302.12041_4

[22] Breier, J., & Hudec , L. (2012). Towards a Security Evaluation Model Based on Security Metrics. Proceedings of the 13th International Conference on Computer Systems and Technologies - CompSysTech'12 (pp. 87 - 94). New York, USA: ACM. doi:10.1145/2383276.2383291

[23] Brenner, S. W. (2004). Toward a Criminal Law for Cyberspace: Product Liability and Other Issues. University of Pittsburgh School of Law Journal of Technology Law and Policy, 5, 1 - 105.

[24] Brenner, S. W. (2007). The History of Information Security: A Comprehensive Handbook. Amsterdam, The Netherlands: Elsevier. doi:https://doi.org/10.1016/B978-044451608-4/50026-2

[25] Brenner, S. W. (2013). Bits, Bytes, and Bicycles: Theft and Cyber Theft. New England Law Review, 47(1), 817 - 859.

[26] Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. US Department of Defense.

[27] Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & Oliveira, R. d. (2013). Your Browsing Behavior for a Big Mac: Economics of Personal Information Online. Proceedings of the 22nd international conference on World Wide Web (pp. 189 - 200). Rio de Janeiro, Brazil: ACM.

[28] Center, I. T. (2019). End of Year Data Breach Report. California, USA.

[29] Chen, X.-Z., Qing-Hua, Z., Xiao-Hong, G., & Chen-Guang, L. C.-G. (2006). Quantitative Hierarchical Threat Evaluation Model for Network Security. Journal of Software, 17(4), 885 - 897. doi:10.1360/jos170885

[30] Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005). Towards A Theory Of Insider Threat Assessment. International Conference on Dependable Systems and Networks (DSN'05) (pp. 108 - 117). Yokohama, Japan: IEEE. doi:10.1109/DSN.2005.94.

[31] Cisco. (2010). Cisco Annual Security Report 2010. California, USA .

[32] Consolvo, S., & Walker, M. (2003, April). Using the experience sampling method to evaluate ubicomp applications. IEEE Pervasive Computing, 2(2), 24 - 31. doi:https://doi.org/10.1109/MPRV.2003.1203750

[33] Coopersmith, J. C. (2009). The History of Information Security: A Comprehensive Handbook (Review). Maryland, USA: Johns Hopkins University Press. doi:https://doi.org/10.1353/tech.0.0193

[34] Council, C. (2018). ISO 27001 vs NIST Cybersecurity Framework. Retrieved January 08, 2020, from https://blog.compliancecouncil.com.au/blog/iso-27001-vs-nist-cybersecurity-framework

[35] CrowdStrike. (2020). Global Threat Report.

[36] Davies, H. (2015). Ted Cruz using firm that harvested data on millions of unwitting Facebook users. (Guardian, Ed.) Retrieved July 31, 2021, from https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

[37] De Zan, , T., d'Amore , F., & Di Camillo, F. (2016). The Defence of Civilian Air Traffic Systems from Cyber Threats. Rome, Italy: Istituto Affari Internazionali.

[38] Dean, K. (2000). The epidemic of cyberstalking Wired News. Retrieved December o4, 2020, from http://www.wired.com/news/politics/0,1283,35728,00.html

[39] DOJ, U. S. (2018). Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps. Retrieved July 31, 2021, from https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

[40] Ebrahimi, F., Tushev, M., & Mahmoud, A. (2020). Mobile app privacy in software engineering research: A systematic mapping study. Information and Software Technology, 1 - 6. doi:10.1016%2Fj.infsof.2020.106466

[41] Ekrem , D., Buyukkaya , A., & Elikucuk , I. (2013). Bank, A Novel and Successful Credit Card Fraud Detection System Implemented in a Turkish. IEEE 13th International Conference on Data Mining Workshops (ICDMW) (pp. 162 - 171). Texas Usa: IEEE.

[42] Elinor, M. (2009). Report: Hackers broke into FAA air traffic control systems. Retrieved July 31, 2021, from https://www.cnet.com/tech/services-and-software/report-hackers-broke-into-faa-air-traffic-control-systems/

[43] Ellison, L. (1999). Cyberspace 1999: Criminals, Criminal justice and the ınternet. . Fourteenth BILETA Conference. York, UK. Retrieved December 04, 2020, from http ://www.bileta.ac.uk/99papers/ellison.html

[44] ENISA. (2020). ENISA Threat Landscape through the years. Retrieved December 09, 2020, from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

[45] Enoch, S. Y., Hong, J. B., Ge, M., & Kim, D. S. (2017). Composite Metrics for Nework Security Analysis. Software Networking 2017, 137 - 160. doi:10.13052/jsn2445-9739.2017.007

[46] ESET. (2010). Cybercrime Coming of Age. Bratislava, Slovakia.

[47] Feng, Z., Li, X., Ren, Y., Cao, Y., & Xu, G. (2017). Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things. IEEE Access, 5(1), 21046 - 21056. doi:10.1109/ACCESS.2017.2734681.

[48] Ficcoa,, M., Chora, M., & Kozik, R. (2017). Simulation Platform for Cyber-Security and Vulnerability Analysis of Critical Infrastructures. Journal of Computational Science, 22, 179 - 186. doi:10.1016/j.jocs.2017.03.025

[49] Field, M. (2017, November 6). The NHS cyber-attack. Retrieved from Acronis.com: https://www.acronis.com/en-eu/articles/nhs-cyber-attack/

[50] nklea, K. M., & Theohary, C. A. (2012). Cybercrime: conceptual issues for congress and US law enforcement. Wahington USA: Congressional Research Service, Library of Congress.

[51] Forum, W. E. (2015). Partnering for Cyber Resilience: Principles and Guidelines. Retrieved December 04, 2020, from https://www.weforum.org/reports/partnering-cyber-resilience-principles-and-guidelines

[52] Fraunholz, D., Krohmer, D., Anton, S. D., & Schotten, H. D. (2017). Investigation of Cyber Crime Conducted by Abusing Weak or Default Passwords with a Medium Interaction Honeypot. International Conference on Cyber Security And Protection Of Digital Services (Cyber Security) (pp. 1 - 7). London, UK: IEEE. doi:10.1109/CyberSecPODS.2017.8074855

[53] Fumagalli, A. (2011). TWENTY THESES ON CONTEMPORARYCAPITALISM (COGNITIVE BIOCAPITALISM). Journal of the Theoretical Humanities, 16(3), 7 - 17. doi:1080%2F0969725X.2011.626555

[54] Hakhroo, B. P. (2020, November). A Study on the types of Cyber Crimes and Cyber attacks in India. International Journal of Creative Research Thoughts, 8(11), 1257 - 1260.

[55] Harrell, E., & Langton, L. (2013). Victims of Identity Theft, 2012. (B. o. Statistics, Ed.) Retrieved July 31, 2021, from https://bjs.ojp.gov/content/pub/pdf/vit12.pdf

[56] Heickerö, R. (2014). Cyber Terrorism: Electronic Jihad. Strategic Analysis, 38(4), 556. doi:http://dx.doi.org/10.1080/09700161.2014.918435

[57] Herjavec, R. (2019, July 18). Cybersecurity CEO: The History Of Cybercrime, From 1834 To Present. Retrieved December 02, 2020, from https://www.herjavecgroup.com/history-of-cybercrime/

[58] Idika , N., & Bhargava, B. (2012). Extending Attack Graph-Based Security Metrics and Aggregating Their Application. IEEE Transaction on Dependaple and Secure Computing, 9(1), 75 - 85.

[59] Imperva. (2014). 2014 Cyberthreat Defense Report NorthAmerica and Europe. CyberEdge Group.

[60] Institute, P. (2014). Cost of a data breach study. IBM.

[61] Institute, S. C. (2012). Cost of Data Breach Study: Global Analysis. New York, USA: Ponemon Institute.

[62] ISO, 2. (2017). ISO 27001 The International Information Security Standard. Retrieved January 08, 2021, from https://www.itgovernanceusa.com/iso27001

[63] Iwuchukwu, U. C., Atimati, E. E., & Ndukwe , C. I. (2017). The State of Clod Computing in Nigeria. Journal of Electrical and Electronics Engineering, 84 - 93. doi:http://dx.doi.org/10.9790/1676-1203028493

[64] Jaquith, A. (2007). Security Metrics: Replacing Fear, Uncertainty, and Doubt. Boston, USA: Addison-Wesley, Pearson Education.

[65] Jibao, L., Huiqiang , W., & Liang, Z. (2006). Research on Network Security Situation Awareness Model. Journal of Computer Research and Development, 43(2), 5 - 9.

[66] Jibao, L., Huiqiang, W., & Shuang, J. (2007). Study of network security situateion awarenesss system based on Netflow. Application Research of Computers, 24(8), 167 - 169 ,172.

[67] Karakilic, E. (2019). Rethinking intellectual property rights in the cognitive and digital age of capitalism: An autonomist Marxist reading. Technological Forecasting & Social Change, 147(1), 1 - 9. doi:10.1016/j.techfore.2019.06.007

[68] Kaspersky. (2019). Kaspersky Security Bulletin 2019. Statistics. Moscow, Russia.

[69] KCC, K. C. (2016). Home Depot Breach Settlement. Retrieved July 31, 2021, from http://www.homedepotbreachsettlement.com/

[70] ttichaisaree, K. (2017). Public International Law of Cyberspace. Switzerland: Springer International Publishing. doi:DOI 10.1007/978-3-319-54657-5_8

[71] Koch, R., & Golling, M. (2018). The Cyber Decade: Cyber Defence at a X-ing Point. 10th International Conference on Cyber Conflict (CyCon) (pp. 159 - 186). Talinn, Estonia: IEEE. doi:https://doi.org/10.23919/CYCON.2018.8405016

[72] Kokolakis, S. (2015, July). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64(1), 1 - 29. doi:10.1016%2Fj.cose.2015.07.002

[73] Kundu, A., Ghosh, N., Chokshi, I., & Soumy, G. K. (2012). Analysis of attack graph-based metrics for quantification of network security. Annual IEEE India Conference (INDICON) (pp. 530 - 535). Kochi, India: IEEE. doi:10.1109/INDCON.2012.6420675.

[74] Lacramioara, B., & Popescu, M. (2011). Credit Card Fraud. The USV Annals of Economics and Public Administration, 11(1), 81 - 85.

[75] Langweg, H. (2006). Framework for malware resistance metrics. Proceedings of the 2nd ACM workshop on Quality of protection (QoP) (pp. 39 -44). Virginia, USA: ACM. doi:10.1145/1179494.1179503

[76] Laughren, J. (2000). Cyberstalking awareness and education. Retrieved December 04, 2020, from http://www.acs.ucalgary.ca/~dabrent/380/webproj/jessica.html

[77] Lee, P. (2020, January 07). Iran attack: how Reaper drones really carry out airstrikes. Retrieved from Theconversation.com: https://theconversation.com/iran-attack-how-reaper-drones-really-carry-out-airstrikes-129411

[78] Lee, R. M. (2015A, February 17). Threat Intelligence in an Active Cyber Defense (Part 1). Retrieved January 16, 2020, from https://www.recordedfuture.com/active-cyber-defense-part-1/

[79] Lee, R. M. (2015B, February 17). Active Cyber Defense Cycle. Retrieved January 16, 2020, from http://www.irongeek.com/i.php?page=videos/bsideshuntsville2015/active-cyber-defense-cycle-robert-m-lee

[80] Lei, L., Huiqiang, W., & Ying, L. (2009). Evaluation method of servicelevel network security situation based on fuzzy analytic hierarchy. Journal of Computer Applications, 29(9), 2327 2335. doi:10.3724/sp.j.1087.2009.02327

[81] Lemos, R. (2003, November 25). The Computer Virus - no cures to be found. Retrieved December 03, 2020, from http://news.zdnet.com/2100-1009_22-5111442.html

[82] Levy, S. (2010). Hackers: Heroes of the Computer Revolution. Boston, Massachusetts, USA: O'Reilly.

[83] Lewis, S., Fremouw, W., & Ben , K. (2001). An ınvestigation of the psychological characteristics of stalkers: Empathy, problem-solving, attachment. Journal of Forensic Sciences, 46(1), 808 - 812.

[84] Li, W., & Vaughn, R. B. (2006). Cluster Security Research Involving the Modeling of Network Exploitations Using Exploitation Graphs. Sixth IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2006). Singapore: IEEE. doi:10.1109/CCGRID.2006.1630921

[85] Lim, B. (2014). Aviation Security: Emerging Threats from Cyber Security in Aviation – Challenges and Mitigations". Journal of Aviation Management, 84.

[86] Lucarelli , S., & Vercellone, C. (2014). The Thesis of Cognitive Capitalism. New Research Perspectives. An Introduction. An introduction. Knowl. Cult., 1(4), 15 - 28.

[87] Maghrabi, L., Pfluegel, E., Al-Fagih, L., Graf, R., Settanni, G., & Skopik, F. (2017). Improved Software Vulnerability Patching Techniques Using CVSS and Game Theory. International Conference on Cyber Security And Protection Of Digital Services (pp. 1 - 6). London, UK: IEEE. doi:10.1109/CyberSecPODS.2017.8074856

[88] Maizlish, B., & Handler, R. (2005). IT Portfolio Management: Step-by-Step. New Jersey, USA: John Wiley & Sons.

[89] Malik, J. K., & Choudhury, S. (2019). llegal access to a computer system: The dark truth of our society. Journal of Information and Computational Science, 9(12), 432 - 447.

[90] Mandt, E. (2017). Integrating Cyber-Intelligence Analysis and Active Cyber-Defence Operations. Journal of Information Warfare, 16(1), 31 - 48.

[91] Maria, K., de Leeuw, M., & Bergstr, J. (2007). The History of Information Security: A Comprehensive Handbook. Amsterdam, Netherlands: Elsevier Science.

[92] McMullan, J. L., & Rege, A. (2013). Online crime and internet gambling. Journal of Gambling Isuues, 24(1), 54 - 85.

[93] Miguel, P. F., & Goncalves, N. (2015). Illegal access to information systems and the Directive. International Review of Law, Computers & Technology, 29(1), 50 - 62. doi:http://dx.doi.org/10.1080/13600869.2015.1016278

[94] Mitnick, K. (2004). Fourth Profile. Australia. Retrieved December 2020, 03, from http://www.zdnet.com.au/insight/security/0,3902376439116620-5,00.htm

[95] Mozzaquatro , B. A., Agostinho, C., Goncalves , D., Martins , J., & Jardim-Goncalves, R. (2018). An Ontology-Based Cybersecurity Framework for the Internet of Things. Sensors, 18(9), 3053. doi:10.3390/s18093053

[96] Negri, A., Hardt, M., & Zolo, D. (2008). Reflections on empire. Cambridge, UK: Polity Press. Retrieved December 04, 2020

[97] Nemlioglu, I. (2019). A Comparative Analysis of Intellectual Property Rights: A case of Developed versus Developing Countries. Procedia Computer Science, 158(1), 988 - 998. doi:10.1016/j.procs.2019.09.140

[98] NIST, N. (2018, April). Framework for Improving Critical Infrastructure Cybersecurity. doi:10.6028/NIST.CSWP.04162018

[99] Ogilvie, E. (2000). Cyberstalking, trends and ıssues in crime and criminal justice. Retrieved December 04, 2020, from http://www.aic.gov.au

[100] Ortalo, R., Deswarte, Y., & KaaÃniche, M. (1999). Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering, 25(5), 633 - 650. doi:10.1109/32.815323.

[101] PAPATHANASAKI, M., DIMITRIOU, G., MAGLARAS, L., VASILEIOU, I., & JANICKE, H. (2018, August). From Cyber Terrorism to Cyber Peacekeeping: Are we there yet? ACM Transactions on Graphics , 37(4), 1 - 7. doi:https://doi.org/10.1145/1122445.1122456

[102] Paulre, B. (2000). From the “New economy” to cognitive capitalism. Association Multitudes.

[103] Payne, B. K., & Hadzhidimova, L. (2018). Cybersecurity and Criminal Justice: Exploring the Intersections. International Journal of Criminal Justice Sciences, 13(2), 385 - 404. doi:10.5281/zenodo.2657646

[104] Raymond, E. S. (2000). A Brief History of Hackerdom. Retrieved December 02, 2020, from http://catb.org/~esr/writings/hacker-history/hacker-history.html

[105] Robert , W. J., & Wood, R. T. (2007, August 31). Internet Gambling: A Comprehensive Review and Synthesis of the Literature. Ontario, Canada. Retrieved 12 03, 2020, from https://hdl.handle.net/10133/432

[106] Roesner, F., Kohno, T., & Weth, D. (2012). Detecting and Defending Against Third-Party Tracking on the Web. Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation (pp. 12 - 15). California, USA: USENIX Association.

[107] Rost, J., & Glass, R. L. (2011). The Dark Side of Software Engineering: : Evil on Computing Projects 1st Edition. John Wiley & Sons.

[108] Saleem, M. (2019). Brexit Impact on Cyber Security of United Kingdom. International Conference on Cyber Security and Protection of Digital Services (Cyber Security). Oxford, England: IEEE. doi:10.1109/CyberSecPODS.2019.8885271

[109] Sallhammar, K., Helvik , B. E., & Knapskog, S. J. (2006). Towards a Stochastic Model for Integrated Security and Dependability Evaluation. First International Conference on Availability, Reliability and Security (ARES'06) (pp. 8, 165). Vienna, Austria: IEEE. doi:10.1109/ARES.2006.137.

[110] Savola, R. (2007). Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry. International Conference on Software Engineering Advances (ICSEA 2007) (pp. 60 - 60). Cap Esterel, France: IEEE. doi:10.1109/ICSEA.2007.79.

[111] Scout, I. T. (2019, January 31). “2018 Annual Data Breach Year-End Review.” . Retrieved from https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

[112] SEC, S. a. (2018). Marriott Announces Starwood Guest Reservation Database Security Incident. Retrieved July 31, 2021, from https://www.sec.gov/Archives/edgar/data/1048286/000162828018014745/a2018ex99.htm

[113] Security. (2017). Midyear Cybersecurity Risk Review: Forecast and Remediations. Dublin: iDefense. Dublin. Retrieved July 31, 2021

[114] Security. (2019). Five Factors Influencing the Cybersecurity Threat Landscape. Retrieved July 22, 2021, from https://www.securitymagazine.com/articles/90718-five-factors-influencing-the-cybersecurity-threat-landscape

[115] Shapiro, C., & Varian, H. R. (1999). Information Rules: A Strategic Guide to the Network Economy. Massachusetts, USA: Harvard Business School Press.

[116] Shea, T. (1984). The FBI goes after hackers, InfoWorld.

[117] Shifflet, J. (2005). A Technique Independent Fusion Model for Network Intrusion Detection. Proceedings of the Midstates Conference on Undergraduate Research in Computer Science and Mathematics, (pp. 13 - 19). Indiana USA.

[118] Shinder, D. L., & Tittel, E. (2002). Scene of the Cyber Crime. Massachusetts USA: Syngress Books.

[119] Sienko, C. (2016). The Breach of Anthem Health – the Largest Healthcare Breach in History. Retrieved July 31, 2021, from https://resources.infosecinstitute.com/topic/the-breach-of-anthem-health-the-largest-healthcare-breach-in-history/

[120] Sohal, A. S., Sandhu, R., Sandeep, S. K., & Chang, V. (2017). A cybersecurity framework to identify malicious edge device in fog and cloud-of-things environments. Computers & Security, 340 - 354. doi:10.1016/j.cose.2017.08.016

[121] Solove, D. J. (2002). Conceptualizing Privacy. California Law Revie, 90(1), 1087.

[122] Song, S., & Zhang, Y. (2011). A Novel Extended Algorithm for Network Security Situation Awareness. 2011 International Conference on Computer and Management (CAMAN) (pp. 1 - 3). Wuhan. China: IEEE. doi:10.1109/CAMAN.2011.5778812.

[123] Steel , E., & Fowler, G. A. (2010, October 10). Facebook in Privacy Breach. Retrieved December 06, 2020, from https://www.wsj.com/articles/SB10001424052702304772804575558484075236968

[124] Steel, E., & Valentino-DeVries , J. (2011, March 16). White House to Push Privacy Bill. Wall Street Journal. Retrieved December 06, 2020, from https://www.wsj.com/articles/SB10001424052748704662604576202971768984598

[125] Strike, , C. (2015). Global Threat Report . California USA.

[126] Strike, C. (2020). Global Threat Report.

[127] Taoa, M., Zuob, J., Castiglioned, A., & Palmieri, F. (2016). Multi-layer Cloud Architectural Model and Ontology-based Security Service Framework for IoT-based Smart Homes. Future Generation Computer Systems. doi:10.1016/j.future.2016.11.011

[128] Target. (2013). Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores. Retrieved July 30, 2021, from https://corporate.target.com/releases/target-confirms-unauthorized-access-to-payment-card-datain-u-s-stores.

[129] Technology, N. I. (n.d.). National Vulnerabilty Database. Retrieved December 08, 2020, from https://nvd.nist.gov/

[130] Teoh, S. T., Ma, K.-L., Wu, S. F., & Zhao, X. (2002). Case study: Interactive visualization for Internet security. VIS2002. IEEE Visualization 2002. Proceedings (Cat. No.02CH37370) (p. 505 = 508). BostoN, USA: IEEE. doi:10.1109/VISUAL.2002.1183751

[131] Tham, I. (2018, July 20). Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack. Retrieved from Straitstimes.com: https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

[132] Thompson, D., & Shears, P. (2003). Lottery fraud: Nothing new under the sun. Journal of Gambling Issues, 9(9), 7 - 15.

[133] Touryalai, H. (2018). World's Largest Hotels 2018: Marriott Dominates, Hyatt & Accor Rise. (Forbes, Ed.) Retrieved July 30, 2021, from

https://www.forbes.com/sites/halahtouryalai/2018/06/06/worlds-biggest-hotels-2018/?sh=732d6b3647c7

[134] Tsakalidis, G., Vergidis , K., & Madas , M. (2018). Cybercrime Offences: Identification, Classification and Adaptive Response. 5th International Conference on Control, Decision and Information Technologies (pp. 470 - 476). Thessaloniki, Greece: IEEE.

[135] Tsakalidis, G., Vergidis, K., & Petrido, S. (2019). A Cybercrime Incident Architecture with an Adaptive Response Policy. Computer and Security, 83, 22 - 37.

[136] Vadza, K. C. (2013, May). Cyber Crime & its Categories. Indian Journal of Applied Research, 3(5), 130 - 135.

[137] Valentino-DeVries, J. (2010, July 31). What They Know About You. Retrieved December 06, 2020, from https://www.wsj.com/articles/SB10001424052748703999304575399041849931612

[138] Vercellone, C. (2007). From Formal Subsumption to General Intellect: Elements for a Marxist Reading of the Thesis of Cognitive Capitalism. Historical Materialism, 15(1), 13 - 36.

[139] Verizon. (2020). Data Breach Investigations Report 2020. Verizon.

[140] Viano, E. C. (2017). Cybercrime, Organized Crime, and Societal Responses. New York. USA: Springer .

[141] Volovelsky, U., & Raynzilber, R. (2013). The liability of website owners for defamation in Israel: A challenge yet to be solved? Computer Law & Security Review, 29(5), 590 - 600. doi:10.1016/j.clsr.2013.07.011

[142] Wang, H. (2006). Survey of Network Situation Awareness System. Computer Science, 33(1), 5 - 10.

[143] Wang, L., Islam, T., Long, T., & Singh, A. (2008). An Attack Graph-Based Probabilistic Security Metric. Proceedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (pp. 283 - 296). London, UK: Springer. doi:10.1007/978-3-540-70567-3_22

[144] Wang, L., Singhal, A., & Jajodia, S. (2007). Toward Measuring Network Security Using Attack Graphs. Proceedings of the 21st annual IFIP WG 11.3 working conference on Data and applications (pp. 98 - 112). Californi, USA: ACM. doi:10.1145/1314257.1314273

[145] Wang, L., Singhal, S., & Jajodia, S. (2007). Toward Measuring Network Security Using Attack Graphs. Proceedings of the 2007 ACM workshop on Quality of Protection (QoP) (pp. 49 - 54). Virginia, USA: ACM. doi:10.1145/1314257.1314273

[146] Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. Pacific-Basin Finance Journal, 57(1), 1 - 12. doi:10.1016/j.pacfin.2019.101173

[147] Warren, S. D., & Brandeis, L. D. (1890). The right to privacy, Harv. Law Rev. 4 (5) (1890) 193–220. Harvard Law Review, 4(5), 193 - 220.

[148] Watson, M. (2019). Top 4 cybersecurity frameworks. Retrieved January 08, 2021, from https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks

[149] Westin, A. F. (1968). Privacy And Freedom. Washington and Lee Law Review, 25(1), 1 - 6.

[150] Wheatley, S., Maillart, T., & Sornette, D. (2015). The Extreme Risk of Personal Data Breaches & The Erosion of Privacy. The European Physical Journal, 89(1), 1 - 12. doi:http://dx.doi.org/10.1140/epjb/e2015-60754-4

[151] Williams, R. J., Wood, R. T., & Park, J. (2012). International Handbook of Internet Gambling. London, UK: Routledge.

[152] Wu , C., & Wang, J. (2019). Analysis of Cyberterrorism and Online Social Media. 4th International Conference on Modern Management, Education Technology (pp. 16 - 39). Guangzhou, Zhuhai, China, Singapore: Atlantis Press.

[153] Xath, C. (2012). The State of Cloud Computing Around the World: South Africa. Retrieved July 07, 2021, from https://cloudtimes.org/2012/10/08/the-state-of-cloud-computing-around-the-world-south-africa/

[154] Ying, L., Huiqiang, W., & Jibao, L. (2007). A Method of Network Security Situation Awareness Based on Rough Set Theory. Journal of Computer Science, 34(8), 95 - 97, 147.

[155] Zhou, F., Shi, R., Zhao, Y., & Huang, Y. (2013). NetSecRadar: A Visualization System for Network Security Situational Awareness. In Cyberspace Safety and Security (pp. 403 - 416). Springer. doi:10.1007/978-3-319-03584-0_30

[156] Zolfagharifard, E. (2014). Hackers are a serious threat to aircraft safety': Aviation chiefs warn of the devastating consequennces of a cyber-attack. Daily Mail. Retrieved July 31, 2021, from https://www.dailymail.co.uk/sciencetech/article-2869827/Hackers-threat-aircraft-safety-Aviation-chiefs-warn-devastating-consequences-cyber-attack.html