SEUSL

Sri Lankan Journal of Technology

Research

Open Access

SLJoT
2021 Sp Issue 39-45
ISSN 2773-6970

Guidelines and Impact of COVID-19 on Cybersecurity: A Model for Protecting Businesses in the Digital Universe

Mahathelge Nicholas Ruwan Dias[1*] and Niresh Eliatamby[2]

[1]Othman Yeop Abdullah Graduate School of Business (OYAGSB) University Utara Malaysia, Malaysia
[2]School of Management, Cardiff Metropolitan University, United Kingdom

[*]Corresponding Author: Drmaha0707@gmail.com

Received: 02-05-2021 ∗ Accepted: 15-07-2021 ∗ Published Online: 15-09-2021

***Abstract*—**The COVID-19 Pandemic significantly increased the use of information and communication technology as governments, institutions and companies worldwide were obliged to move to a work-from-home model in order to ensure the survivability of their businesses and other operations. This in turn led to a significant increase in cyberattacks due to the larger number of operations that were moved from physical space to cyberspace. The pandemic resulted in the heightened importance and awareness of the need for IT security. Companies learned the hard way during the pandemic that a business could be destroyed by a single cyberattack and that the concept of IT security entailed more than simply hiring an IT manager and fixing a virus guard. This also resulted in much confusion as to the real cost and the level of sophistication that is necessary to safeguard an institution's IT operations. This paper is intended to provide guidance to IT professionals and entrepreneurs with regard to the practical steps that should be taken to protect one's business in cyberspace. In particular, it explores fundamentally simple practices such as vulnerability testing, patching and correct configurations, by which as much as 80% of data breaches can be prevented. The paper uses Sri Lanka as a case study and analyses contemporary data published by the Sri Lanka Computer Emergency Response Team.

***Keywords*—**Cybersecurity, Cyber-attacks, Covid-19, End-user Model, Digital

I. Introduction

Cyberthreats have shown a clear increasing trend, resulting in a similar need to respond through greatly enhanced cybersecurity measures. As many as 68% of business leaders feel their cybersecurity risks are increasing. Worldwide spending on cybersecurity is projected to reach $133.7 billion in 2022 (Smyrlis et al., 2020). In the first half of 2019, data breaches exposed 4.1 billion records, placing at risk the private data of billions of persons (Tejay and Paul, 2020). The main motivation for cyberattacks and data breaches appears to be financial (Poyraz et al., 2020). As many as 71% of breaches were financially motivated and 25% were motivated by espionage (Fielding, 2020). The methods of cyberattacks have varied significantly, with 52% of breaches having featured hacking, 28% having involved malware and 32–33% included phishing or social engineering (Jartelius, 2020). Common methods of data breaches are weak and stolen credentials, through the use of passwords, back doors, application vulnerabilities, malware, social engineering, multiple permissions, insider threats, improper configuration and user error (Liu et al., 2018). Email remains the preferred mode of entry for cyberattacks, with 92% of malware being delivered by email (Alladi, Chamola and Zeadally, 2020). Meanwhile, confidence in available cybersecurity measures remains weak and the classic anti-virus approach may not continue to grow as many new threats cannot be recognized (Fleshman et al., 2018), for example, a fraudulent email being sent from a senior employee to an in-house employee asking for information about a customer or bank account. The FBI reports that the US losses were over $1.7 billion in 2019 in this type of fraud (Richardson, 2020). The use of digital communication technologies has proliferated in the context of the current pandemic, which has both increased the profile of cyber security and its importance in supporting modern social, economic and political life (Carrapico and Farrand, 2020).

The literature review was carried out in a wide-ranging manner to gather literature on cybersecurity on a worldwide basis, but focused on Sri Lanka as a case study with analysis of available literature. Due to restrictions on physical travel required by the COVID-19 pandemic, the Literature Review was carried out online.

A. Internal Threats

Despite almost two decades of research to detect and prevent insider threats, the progress of modern networks has rapidly outperformed these efforts. As a result, the victims of malicious activity continue to report huge losses, most of whom are not aware of their risk until harmful behaviour has taken place. This may be due to one or more of the following reasons - most of the solutions rely solely on an audit data source to decrease the insight into threats; conventional data analysis counts too much on domain information in removing or establishing functions; and the existing solutions fail to focus on early evidence of malicious insiders (Liu et al., 2018). Company employees are consistently identified as one of the main vulnerabilities that compromise company and client financial data. This threat increases with the increase in the number of employers working from home (WFH) (Ahmad, 2020). The three main reasons are using personal devices lacking the same security as company issued devices, forwarding sensitive business and client information to personal accounts, and failure of conference calls (example: ZOOM Bombing) (Putz and Pernul, 2019; Secara, 2020; Škiljić, 2020).

B. External Threats

The goals of bad actors include obtaining access to organisation systems, stealing personal information and locking down computers with ransomware. Typical malicious transactions include imposter scam-advantage on negative situations, e.g., sending emails pretending to be from WHO to share new information about Coronavirus, and sending emails as though they are from government agencies or officials to collect personal information. Another often used external threat is product scams - fake shops and websites, coronavirus vaccines, surgical masks (trying to steal personal information. Other external threats are cybercriminal attacks, phishing attacks, spreading malware, stealing login credentials, and fake calls.(Keshavarzi and Ghaffary, 2020).

C. Application and Networking Attacks

The inbound attack is the first step towards a deeper deepening of traditional defections, such as next generation firewalls and antivirus systems. The conventional protection of the network is supposed to be bypassed in advanced cyber-attacks. Cyber-attacks of the next generation target particular individuals and organizations to steal information. Bad actors also use various channels such as the Internet, email, and malicious files and quickly respond to voided vulnerabilities and other vulnerabilities (Abd Elazim, Sobh and Bahaa-Eldin, 2018; Gao et al., 2018).

D. Advanced Cyber Attacks

Advanced cyber-attacks find success because of their planning, methodology, and careful design. In such attacks, malware settles in a system, tries to hide, finds vulnerabilities in the network, disables security measures of the network, infects more terminals and other instruments, returns to command and control servers, and waits for instructions on starting network data extraction. By the time most organizations realize that they have been attacked, in reality, the attacks have been taking place for weeks, months, or even years. Most traditional cyber security defence measures, such as AV firewalls or next generation firewalls, do not use signature techniques or pattern-based threats and do not track malware CnC call-backs. Advanced cyber-attacks take many forms, including viruses, Trojans, spyware, rootkits, phishing spears, malicious attachments, and download drives (Conti, Dargahi and Dehghantanha, 2018; Bhatnagar, Som and Khatri, 2019). Advanced attacks target information about companies and users including personal information and other information, proprietary or confidential. It reduces security device effectiveness substantially through changes of settings and configurations, installation of additional software and providing access to third parties. These forms of attacks can also execute arbitrary code on devices remotely to enable hackers to control the device completely (Boiko, Shendryk and Boiko, 2019).

E. International conventions on cybersrime

Despite a quarter century of Internet connectivity, global cooperative efforts to combat cybercrime remain at an early stage, with progress towards worldwide agreements and conventions being very slow, especially in comparison to the rapid rate of development and evolution of the ICT industry and cybercrime. Many globally relevant standards have been driven by the European Union, but most nations continue to rely on their own legislation (Koziarski and Lee, 2020).

F. Budapest Convention on Cybercrime 2001

Arguably the first integrated global effort to combat cybercrime, the Budapest Convention was drawn up by the Council of Europe and came into force in 2004. As of April 2021, it had been ratified by 65 nations. However, several important nations have declined to join including Russia, China, and India. It has gone a long way toward harmonizing laws of participatory states, improving investigative methodologies into cybercrime, and generally increasing cooperation among nations. The wide range of subjects it deals with includes cyber fraud, internet child pornography, and internet copyright violations (Wicki-Birchler, 2020).

G. European Union General Data Protection Regulation (GDPR) 2016

General Data Protection Regulation (EU) 2016/679 superseded the outdated Data Protection Directive 95/46/EC. It introduced one standard for data protection within the EU and the European Economic Area and is also of relevance to the transfer of data outside of Europe in as much as it affects any European individual or entity (Yan and Chua, 2020).

H. European Union NIS Directive 2016

Introduced in 2016, the Directive on Security of Network and Information Systems required the harmonization of network information systems into national laws throughout the EU by 2018 (Markopoulou, Papakonstantinou and de Hert, 2019).

I. Sri Lankan legislation on cybersecurity

Sri Lanka has introduced a wide range of comprehensive Acts that have facilitated the prevention, criminalization, investigation, and prosecution of cybercrime. However, the regulatory framework is based on a governmental and institutional point of view and there remain gaps in areas such as personal data protection that are in the process of being addressed (Eliatamby, 2020).

Evidence (Special Provisions) Act, No. 14 of 1995: This Act amended court procedures to provide for the admissibility in court of any evidence contained in electronic formats, including audio-visual recordings and translations of evidence in machine language.

Intellectual Property Act, No 36 of 2006: A powerful Act that provides protection for software, trade secrets, and integrated circuits.

Payment Devices Frauds Act, No. 30 of 2006: This Act is of particular relevance to the banking industry as it criminalizes the use of counterfeit and unauthorized payment devices or unauthorized use of genuine payment devices.

Computer Crimes Act, No. 24 of 2007: A powerful piece of legislation that criminalizes any act of ‘hacking’ in Sri Lanka or outside Sri Lanka by an individual, group or institution; of unauthorized access to a computer, computer programme, data, or information including any downloads; modification, alteration or deletion of information, the introduction of viruses, copying of information, or interception of the information while it is being transmitted. It also criminalizes the use of a computer to harm national security, the national economy, or public order, which provides authorities with very broad powers. It also criminalizes the unauthorized distribution of information including passwords. The Act prescribes a variety of penalties for transgressions including fines, prison terms, and compensation. It also authorizes law enforcement authorities to call upon any expert for assistance, including universities.

Level-1 Mutual Assistance in Criminal Matters (Amendment) Act, No. 24 of 2018 This Act authorizes Sri Lankan law enforcement agencies to obtain assistance from any foreign authority to carry out investigations on crimes committed digitally. This includes requests for the arrest of suspects living in other nations’ jurisdictions.

Personal Data Protection Bill At the present time, there is a huge vacuum in Sri Lankan cyber law in the area of personal data protection. A Bill was drafted by the Ministry of Digital Infrastructure Information Technology in 2019, but has not yet been brought before parliament.

II. CYBER SECURITY CHALLENGE

Cyber threats have been continuously evolving since the advent of the first cyberthreat. The COVID-19 era is no exception and poses a major challenge for cybersecurity. It is important that each business leader takes measures to ensure that their organisation continues to run securely and that remote employees have a seamless home working experience. Security experts can help organizations with the most urgent challenges associated with smartphones, tablets, laptops, and other remote infrastructures when they require the right strategy or a comprehensive security team (Ahmad, 2020; Burton and Lain, 2020; Caviglione et al., 2021).

A. Cybersecurity in Sri Lanka

As a national contact point for all information security related matters, the Sri Lanka Computer Emergency Response Team (SLCERT) receives a significant number of incidents/complaints related to the country’s national information domain, from both domestic and foreign entities. Incidents of social networking, email vulnerabilities, phishing, compromise of websites, malware, malicious software and ransomware, breaches of privacy, financial fraud, uniform IPs affected from information collected on automated systems run by international organisations, are some of the complaints to SLCERT. In recent years, Sri Lanka’s computer equipped households have grown to 23.5% and 21.3% are internet users. In addition, the country’s computer literacy rate has increased over the last decade which has also brought about an increase in abuse and misuse (Kulathunga, 2019).

A summary of data related to cyber security obtained during 2019 by SLCERT is given below:

- During 2019 reports of the number of cases of abuse of personal data increased.
- Reports of malicious software and ransomware increased during 2019, mainly in relation to confidential data from both individuals and organizations being made unavailable by encryption, deletion or alteration.
- A significant number of diversion websites had been registered in 2019 which targeted government and private sector organisations.
- The vast majority of incidents were related to social media, of which the highest number were in relation to Facebook usage.

III. METHODOLOGY / METHODS

Sri Lanka is used as a case study with data reported by the government authority SLCERT being analysed for the purposes of this paper. Prior to the advent of the pandemic, Sri Lanka recorded a low level of internet penetration due to a variety of reasons including the high cost of ICT infrastructure and low levels of ICT awareness. This underwent a significant metamorphosis following the introduction of a work-from-home culture in as much as it was possible in a state with a low level of industrialisation and technology. This in turn led to a significantly increased number of cyberattacks, as the growth in ICT usage coupled with a low level of awareness of global best practices in cybersecurity.

Compared to the previous year 2019, incidents related to cyber-security reported to the Sri Lanka Computer Emergency Readiness Team (SLCERT)(CERT|CC, 2020), the state governing authority on cybercrime, have declined in 2020, totalling 2,079, as shown in Table 1, while in 2019 the total reported was 3,123, and in 2018 it was 2,361. But it can be seen that cyber threats to businesses have increased. The increase is attributable to the considerable number of cases of compromise on the website and data protection problems.

Table I: Reported cybersecurity incident cases in Sri Lanka 2017-2020 Source: (CERT|CC, 2020)

Incident Type	**No. of Incidents 2020**	**No. of Incidents 2019**	**No. of Incidents 2018**	**No. of Incidents 2017**
Availability	**1**	**2**	**0**	**0**
DDOS	1	2	0	0
Intrusions	**59**	**175**	**5**	**6**
Account Compromised	5	2	0	0
Defacement	54	168	5	4
Exploiting Known Vulnerability	0	5	0	2
Information Content Security	**1115**	**715**	**693**	**803**
- Unauthorized Access and Modifications to Information	1115	715	693	803
Fraud	**99**	**52**	**12**	**17**
- Copyright	0	1	2	6
- Masquerade	25	14	0	1
- Phishing	8	7	0	0
- Scam	66	30	10	10
Malicious Code	**18**	**28**	**0**	**1**
- Virus	1	1	0	0
- Trojan	5	0	0	0
- Ransomware	12	27	0	1
Abusive Content (Cyber Harassment)	**758**	**1493**	**1411**	**2276**
- Harmful Speech	0	277	0	0
- Fake Accounts	675	944	1244	1880
-Child/Sexual/ Violence	70	238	147	341
- Cyber Bullying & Stalking	13	7	20	55
- Racial	0	27	0	0
Other	**29**	**658**	**240**	**224**
- Incidents which do not fall into one of the given categories	29	658	240	224
Total	**2079**	**3123**	**2361**	**3327**

IV. Results Discussion

Although the overall number of threats has reduced in 2020, it can be seen that the number of business threats increased in 2020 in the areas of Information Content Security and Fraud, while there has been a reduction in personal threats in the categories of Intrusions and Cyber Harassment. in the area of Frauds, both Masquerades and Scams have recorded increases in 2020.

Overall, the level of intrusions in 2020, both business and personal, remains high in comparison to 2018.

It can be deduced that the focus of cyberthreats in Sri Lanka has shifted during the pandemic era from personal to business-oriented threats.

In order to protect the information processed by the organization through compliance with information security policy and the understanding, the cyber security culture can be contextualized in an organizational context to ensure that the needs of regular communication, awareness, training and educational efforts are implemented carefully (Alshaikh, 2020).The researchers have devised the following model, depicted in Fig. 1, by which businesses could strengthen their cybersecurity (Mahathelge Nicholas, 2017; Dias and Eliatamby, 2020).

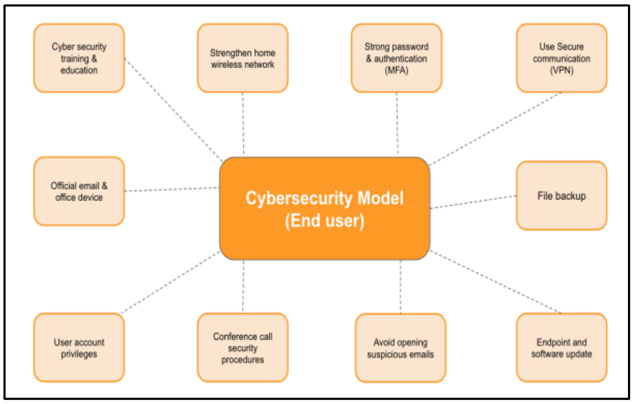
Cyber security training & education
Strengthen home wireless network
Strong password & authentication (MFA)
Use Secure communication (VPN)
Official email & office device
Cybersecurity Model (End user)
File backup
User account privileges
Conference call security procedures
Avoid opening suspicious emails
Endpoint and software update

Figure 1: Recommended cybersecurity model for businesses, Source: (Dias and Eliatamby, 2020).

A. *Recommended Policies Network Actions*

Review policies and procedures and revise as necessary which included using personal devices for corporate use and storing personal credentials in websites.

Review policies and procedures and revise as necessary, including using personal devices for corporate use and storing personal credentials in websites. For the employee who works from home, It is necessary to assess infrastructure. Typically, virtual private network services provide a wide range of protection and enhanced network security services. Users are mandatory to comply with MFA- Multi-Factor authentication to safeguard the user authentication. The organization has to implement a mobile device management (MDM) program to wipe out the mobile data in case users lose the device). The organization has to implement best practices such as temporary vendor access and resign employees (Karmakar, Varadharajan and Tupakula, 2019)

B. *People Vulnerabilities Action*

The organization has to monitored unknown assets on the network. Asset registers are mandatory to update OS patches periodically. They must implement a policy of least privilege and a lack of defense in depth practices (Birkinshaw, Rouka and Vassilakis, 2019).

C. *Protect from Eavesdropping*

Eavesdropping attacks on private conversations or secret contact with people without their permission. Employees have to avoid the same security codes to access the conference call. Furthermore, they have to implement best practices such as one-time pin code creation, meeting identification code, and turn off third party home devices (e.g., Alexa or Google Home) (Richardson, 2020)

D. Actions for outsider threats

System administrators need to deploy or reinforce protective measures to address vulnerabilities. They have to identify vulnerabilities in their current environment, leverage available resources to monitor and identify threats and enforce endpoint protection, sensitive information(Borky and Bradley, 2019). The security team needs to configure email scanning and settings such as SPAM and malware protection of mailboxes, implementing DomainKeys Identified Mail (DKIM) security standard implementing Domain-based Message Authentication secure domain name configuration for the sender policy framework (SPF). The administrator must implement strong authentication for the accessing systems. All password complexity requirements, MFA, and conditional access policies are enforced as a mandatory requirement. Implementing the Multi-Factor Authentication in the organization has to be compulsory to access any system or service. Organisation email security strategy is important to the organization ability to continually analyse threats and monitor trends in traffic.

It is vital to comprehensive protection from Business Email compromise (BEC) threats. BEC is a kind of cyber-criminal e-mail scam that an attacker targets companies to defraud the company. BEC scams have exposed organisations, in potential losses, to billions of dollars. Cyber criminals are threatening phishing, whereby employees or consumers are forced to disclose or transfer data. IT monitoring, user training, comprehension and testing help users get better educated and intelligent (Gupta, Arachchilage and Psannis, 2018; Birkinshaw, Rouka and Vassilakis, 2019; Richardson, 2020; Rouka, Birkinshaw and Vassilakis, 2020).

V. Conclusions

Cybersecurity is comparable to home security or building security, with many levels of threats and the requirement for several layers of defences, e.g., fence, guard dogs, security guards, burglar alarms, lighting, etc. As illustrated in the authors' model, there is no single defence that can provide complete protection, and it takes a diverse range of defence mechanisms to protect a business.

In addition, it is vital that the dynamic nature of the digital universe be taken into consideration, i.e., the defences set up today need to be periodically revisited and constantly upgraded in order to cater to evolving threats. It must be kept in mind that every new protective technique spawns new hacking techniques that are designed to penetrate it. Therefore, countries and businesses must always be a step ahead of cyber criminals in order to keep their operations safe.

However, it is vital that the setting up and/or upgrading of a system of defences be carried out in a systematic manner, as per the authors' model recommended in this paper.

References

Abd Elazim, N. M., Sobh, M. A. and Bahaa-Eldin, A. M. (2018) 'Software Defined Networking: Attacks and Countermeasures', in *2018 13th International Conference on Computer Engineering and Systems (ICCES).* IEEE. doi: 10.1109/ICCES.2018.8639429.

Ahmad, T. (2020) 'Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity', *SSRN Electronic Journal.* doi: 10.2139/ssrn.3568830.

Alladi, T., Chamola, V. and Zeadally, S. (2020) 'Industrial Control Systems: Cyberattack trends and countermeasures', *Computer Communications,* 155. doi: 10.1016/j.comcom.2020.03.007. Alshaikh, M. (2020) 'Developing cybersecurity culture to influence employee behavior: A practice perspective', *Computers Security,* 98. doi: 10.1016/j.cose.2020.102003.

Bhatnagar, D., Som, S. and Khatri, S. K. (2019) 'Advance Persistant Threat and Cyber Spying - The Big Picture, Its Tools, Attack Vectors and Countermeasures', in *2019 Amity International Conference on Artificial Intelligence (AICAI).* IEEE. doi: 10.1109/AICAI.2019.8701329.

Birkinshaw, C., Rouka, E. and Vassilakis, V. G. (2019) 'Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks', *Journal of Network and Computer Applications,* 136. doi: 10.1016/j.jnca.2019.03.005.

Boiko, A., Shendryk, V. and Boiko, O. (2019) 'Information systems for supply chain management: uncertainties, risks and cyber security', *Procedia Computer Science,* 149. doi: 10.1016/j.procs.2019.01.108.

Borky, J. M. and Bradley, T. H. (2019) 'Protecting Information with Cybersecurity', in *Effective Model-Based Systems Engineering.* Cham: Springer International Publishing. doi: 10.1007/978-3-319-95669-$5_1$0.

Burton, J. and Lain, C. (2020) 'Desecuritising cybersecurity: towards a societal approach', *Journal of Cyber Policy,* 5(3). doi: 10.1080/23738871.2020.1856903.

Carrapico, H. and Farrand, B. (2020) 'Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy', *Journal of European Integration,* 42(8). doi: 10.1080/07036337.2020.1853122.

Caviglione, L. et al. (2021) 'Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection', *IEEE Access,* 9. doi: 10.1109/ACCESS.2020.3048319.

CERT|CC (2020) *Sri Lanka CERT Annual Activity Report 2020, Sri Lanka CERT\CC.* Available at: https://www.cert.gov.lk/view?lang=enarticleID=164 (Accessed: 4 June 2021).

Conti, M., Dargahi, T. and Dehghantanha, A. (2018) ‘Cyber Threat Intelligence: Challenges and Opportunities’, in. doi: 10.1007/978-3-319-73951-9_1.

Dias, M. N. R. and Eliatamby, N. (2020) *Covid-19 and cybersecurity: Protecting your business - The Morning - Sri Lanka News, Liberty Publications.* Available at: https://www.themorning.lk/protecting-your-business-in-the-digital-universe/ (Accessed: 4 June 2021).

Eliatamby, N. (2020) *Regulating Social Media in Sri Lanka – A Comparative Study with Selected Jurisdictions.* Cardiff Metropolitan University.

Fielding, J. (2020) ‘The people problem: how cyber security’s weakest link can become a formidable asset’, *Computer Fraud Security,* 2020(1). doi: 10.1016/S1361-3723(20)30006-3.

Fleshman, W. et al. (2018) ‘Static Malware Detection amp; Subterfuge: Quantifying the Robustness of Machine Learning and Current Anti-Virus’, in *2018 13th International Conference on Malicious and Unwanted Software (MALWARE).* IEEE. doi: 10.1109/MALWARE.2018.8659360.

Gao, S. et al. (2018) ‘Security Threats in the Data Plane of Software-Defined Networks’, *IEEE Network,* 32(4). doi: 10.1109/MNET.2018.1700283.

Gupta, B. B., Arachchilage, N. A. G. and Psannis, K. E. (2018) ‘Defending against phishing attacks: taxonomy of methods, current issues and future directions’, *Telecommunication Systems,* 67(2). doi: 10.1007/s11235-017-0334-z.

Jartelius, M. (2020) ‘The 2020 Data Breach Investigations Report – a CSO’s perspective’, *Network Security,* 2020(7). doi: 10.1016/S1353-4858(20)30079-9.

Karmakar, K. K., Varadharajan, V. and Tupakula, U. (2019) ‘Mitigating attacks in software defined networks’, *Cluster Computing,* 22(4). doi: 10.1007/s10586-018-02900-2.

Keshavarzi, M. and Ghaffary, H. R. (2020) ‘I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion’, *Computer Science Review,* 36. doi: 10.1016/j.cosrev.2020.100233.

Koziarski, J. and Lee, J. R. (2020) ‘Connecting evidence-based policing and cybercrime’, *Policing: An International Journal,* 43(1). doi: 10.1108/PIJPSM-07-2019-0107.

Kulathunga, A. (2019) ‘A Comparative Study on Sri Lankan v. European Cybercrime Law in Protecting IT Professionals and Victims of Cyber-attacks’, *SSRN Electronic Journal.* doi: 10.2139/ssrn.3645099.

Liu, L. et al. (2018) ‘Detecting and preventing cyber insider threats: A survey’, *IEEE Communications Surveys Tutorials,* 20(2), pp. 1397–1417.

Mahathelge Nicholas, R. D. (2017) ‘Enterprise security architecture framework (ESAF) for banking industry / Mahathelge Nicholas Ruwan Dias’.

Markopoulou, D., Papakonstantinou, V. and de Hert, P. (2019) ‘The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation’, *Computer Law Security Review,* 35(6). doi: 10.1016/j.clsr.2019.06.007.

Poyraz, O. I. et al. (2020) ‘Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches’, *The Geneva Papers on Risk and Insurance - Issues and Practice,* 45(4). doi: 10.1057/s41288-020-00185-4.

Putz, B. and Pernul, G. (2019) ‘Trust Factors and Insider Threats in Permissioned Distributed Ledgers’, in. doi: 10.1007/978-3-662-60531-8_2.

Richardson, J. (2020) ‘Is there a silver bullet to stop cybercrime?’, *Computer Fraud Security,* 2020(5). doi: 10.1016/S1361-3723(20)30050-6.

Rouka, E., Birkinshaw, C. and Vassilakis, V. G. (2020) ‘SDN-based Malware Detection and Mitigation: The Case of ExPetr Ransomware’, in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT).* IEEE. doi: 10.1109/ICIoT48696.2020.9089514.

Secara, I.-A. (2020) ‘Zoombombing – the end-to-end fallacy’, *Network Security,* 2020(8). doi: 10.1016/S1353-4858(20)30094-5.

Škiljić, A. (2020) ‘Cybersecurity and remote working: Croatia’s (non-)response to increased cyber threats’, *International Cybersecurity Law Review,* 1(1–2). doi: 10.1365/s43439-020-00014-3.

Smyrlis, M. et al. (2020) ‘Cyber Range Training Programme Specification Through Cyber Threat and Training Preparation Models’, in. doi: 10.1007/978-3-030-62433-0_2.

Tejay, G. and Paul, S. (2020) ‘Special Issue Introduction’, *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* 51(1). doi: 10.1145/3380799.3380802.

Wicki-Birchler, D. (2020) ‘The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?’, *International Cybersecurity Law Review,*| 1(1–2). doi: 10.1365/s43439-020-00012-5.

Yan, N. W. J. and Chua, H. N. (2020) ‘A Path Analysis Model to Identify the Effects of Social Media, News Media and Data Breach on Data Protection Regulation Awareness’, in *2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET).* IEEE. doi: 10.1109/IICAIET49801.2020.9257846.