An Analysis of Cybersecurity Architectures

Noluntu Mpekoa
University of Johannesburg, South Africa

noluntum@uj.ac.za

Abstract: The 4th Industrial Revolution has increased high-capacity connectivity, new human-machine interactions largely with IoTs and smart devices. This digital revolution offers incredible conveniences such as the ability for users to access volumes of data, governments can address social challenges, connect remote villages in the country, and more. Once secluded systems are now connected and sharing information. This connectedness also poses some inconveniences as well, whenever a device joins the Internet, it becomes publicly discovered. Once these devices are discovered, they become open to cyberattacks. Cybersecurity has become a crucial part of daily life as cyberattacks have increased over time and have become more and more severe. The challenge that cybersecurity consultants find is the difficulty of measuring cybersecurity efforts in organizations. Another challenge could be finding a cybersecurity architecture that is effective and can fit different situations. The main aim of this study was to develop a comprehensive cybersecurity architecture that can be used by cybersecurity consultants when measuring cybersecurity effectiveness. This study conducted an in-depth literature review on current cybersecurity architectures offered by national and international cybersecurity organizations. The identified cybersecurity architectures that have been developed by other organizations were translated, interpreted, compared, and synthesized and a new cybersecurity architecture is proposed. The proposed cybersecurity architecture has the NIST goals as a foundation and the CIA triad at the center. The proposed cybersecurity architecture has domains such as application and Systems security, Information security, Network security, End-point security, Critical Infrastructure security, Mobile security, Storage security, etc. The proposed cybersecurity architecture seeks to assist cybersecurity consultants in answering questions from executives such as: Are we secure? Are security investments delivering value to the business? What is our preparedness for a cyberattack?

Keywords: Security architecture, Cybersecurity, Security capability domain, Cybersecurity control areas

1. Introduction

The Fourth Industrial Revolution (4IR) has led to an increase in high-capacity connectivity and new human-machine interactions, largely through the Internet of Things (IoT) and smart devices. This digital revolution offers incredible conveniences. Users can access vast amounts of data, governments can address social challenges, and remote villages can connect with the rest of the country. Communities have transitioned into digital spaces, encompassing work, leisure, and commerce (WEF, 2017; Ivanov & Das, 2020). Digital tools in the classroom have provided teachers and students with increased opportunities. Teachers have been pushed to evolve their teaching strategies to support personalized learning, creativity, innovation, and problem-solving, and provide more time for individual instruction. (WTO, 2020). Many businesses suffered during and after COVID-19, with some SMEs closing down. The 4IR has become more affordable and easier to implement, thus providing a viable recovery strategy for many businesses (Ivanov & Dolgui, 2021). PwC in 2018 conducted an annual global CEO survey, where "81% of executives agreed that 4IR technologies created new efficiencies, and 78% agreed that they helped them automate tasks" (PwC, 2018).

Previously isolated systems are now interconnected and sharing data. Möller (2023) states that this connectedness also poses some inconveniences as well, whenever a device joins the Internet, it becomes publicly discovered. Once these devices are discovered, they become open to cyberattacks (Singh & Kumar, 2020; Aphane, 2023). Cybersecurity has become an essential part of our daily lives due to the increasing frequency and severity of cyberattacks. Cybersecurity consultants face a significant challenge in measuring the effectiveness of cybersecurity measures in organizations. Another challenge could be finding a cybersecurity architecture that is effective and can fit different situations (Mbelli & Dwolatzky, 2016; Carcary, Doherty & Conway, 2019).

The main aim of this study was to develop a comprehensive cybersecurity architecture that can be used by cybersecurity consultants when measuring cybersecurity effectiveness. The following section will provide a brief overview of cybersecurity architectures, then followed by the research methodology utilised in this study. The proposed cybersecurity architecture is then presented and followed by the discussion and conclusion.

2. Overview of Cybersecurity Architectures

2.1 Cybersecurity Investment and ROI

The last quarter of 2022 and first quarter of 2023 saw an alarming 18.8% surge in cyberattacks in South Africa (SA). This is a clear indication of the ever-increasing threat of cybercrime and highlights the need for

individuals and organizations alike to take proactive measures to protect their digital assets (Kaspersky, 2023; DA, 2023). The Interpol (2022) report states that South Africa has been labeled as the cybercrime hub of Africa, and hackers on the dark web have shown interest in the country. In 2020, an Accenture report revealed that the country's internet users were less experienced and technically alert (Accenture, 2020). Poor cybersecurity awareness and lack of end-user training have contributed to successful cyberattacks in South Africa (Möller, 2023; Ngoma, Keevy, & Rama, 2021). Table 1 below, demonstrates the extent of imminent cyberattacks in the country, extracted from various sources (Paganini, 2022; DA, 2023)

Table 1: Summary of Cybersecurity Attacks in South Africa

YEAR	ATTACK DETAILS
March 2022	Everest gang demands $200K for data stolen from ESKOM
May 2022	TransUnion cyber-attack – hackers demand R225 million ransom
July 2022	Transnet Port Terminals attack
December 2022	Postbank loses over R18-million to cybercrime attacks
February 2023	Porsche South Africa suffers ransomware attack
April 2023	Justice department loses millions in yet another cyber attack
August 2023	Daily Maverick DDoS attack during BRICS Summit

Cybercrime is one of the biggest business risks in South Africa, and it is predicted that government departments will face an increasing number of attacks. The economy suffers an estimated loss of R2.2 billion per year due to cybercrime (Kaspersky, 2023; Paganini, 2022; Mbelli & Dwolatzky, 2016). Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access (Ivanov & Das, 2020; Singh & Kumar, 2020). Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) have experienced difficulties in justifying cybersecurity investments or expenses (Fowler & Chen, 2017; Hallman *et al.*, 2021; Moore, Dynes & Chang, 2016). Cybersecurity managers and specialists are constantly asked questions by executives such as: Are we secure? Are security investments delivering value to the business? What is our preparedness for a cyberattack? The primary responsibility of CIOs/CISOs is to implement effective cybersecurity measures to prevent attacks that may disrupt or disable the operations of their organization.

2.2 Cybersecurity Architectures

Cybersecurity architectures consist of distinct and comprehensive domains that are separate from each other. The different categories that come under cybersecurity are often referred to as domains. Some people may also call them control areas or capability domains (Roy, Kim & Trivedi, 2010; Möller, 2023). When referring to cybersecurity domains, one is essentially talking about the specific area of cybersecurity being discussed. In simpler terms, a domain refers to a specific category or focus area, especially in cybersecurity. When various cybersecurity domains are integrated, it results in the formation of a Cybersecurity Architecture. Cybersecurity organizations and frameworks define the domains of cybersecurity differently (Möller, 2023, Bokan & Santos, 2021; AlHamdani, 2020). The concept of cybersecurity architecture has many faces, and each framework has its own focus and strengths. To such an extent that, several frameworks exist for cybersecurity architecture, the most popular and common ones are the NIST Framework, Open-Source Architecture and the International Information System Security Certification Consortium, otherwise known as (ISC)2.

Some of these cybersecurity architectures complement each other and may have overlapping features. Application security, physical security, risk assessment, and threat intelligence are some of the most common domains in cybersecurity. Table 2 below lists some of the common cybersecurity architectures.

Table 2: Cybersecurity Domains

NIST Capability Domains	CISSP Certification	GSEC Certification	Open-Source Architecture	Decipher Zone
Access Control	Security and Risk Management	Active Defense	IT Service Security Patterns	Network Security
Security Assessment	Asset Security	Cryptography	IT Application-Level patterns	Cloud Security

NIST Capability Domains	CISSP Certification	GSEC Certification	Open-Source Architecture	Decipher Zone
Awareness & Training	Security Engineering	Defensible Network Architecture	IT Infrastructure Patterns	Application Security
Risk Management	Communications and Network Security	Incident Handling and Response	Central Security Services	Critical Infrastructure Security
Situational Awareness	Identity and Access Management	Linux Security	Governance	End-User Security
Asset Management	Security Assessment and Testing	Security Policy		Disaster Recovery
Media Protection	Security Operations	Web Communication Security		Information security
Maintenance	Software Development Security			Storage Security
Personal Security				Mobile Security
Audit & Accountability				
System & communication protection				
Identification & Authentication				

The task at hand is to design a cybersecurity framework that is both effective and tailored to one's unique situation or organization. The second challenge that Cybersecurity managers and specialists face is creating the best cybersecurity architecture from a diverse range of options.

3. Research Methodology

The main aim of this study was to develop a comprehensive cybersecurity architecture that can be used by cybersecurity consultants when measuring cybersecurity effectiveness. The proposed cybersecurity architecture seeks to assist cybersecurity consultants in answering questions from executives such as: Are we secure? Are security investments delivering value to the business? What is our preparedness for a cyberattack? An in-depth literature study was conducted to have a fundamental understanding of the research problem. A qualitative meta-synthesis methodology to synthesize different cybersecurity architectures was utilised. This process follows the steps in the meta-ethnography approach (Bhattacharyya, 2009; Rajasekar & Verma, 2013; Snyder, 2019). Qualitative meta-synthesis is a technique for synthesizing the findings of qualitative research. The method aims to explain the findings of similar qualitative studies. The result is used as the basis for the design of the proposed comprehensive cybersecurity architecture (Goddard & Melville, 2004). The primary sources of data were derived based on published articles, reviews, and books to gain essential data that assisted in formulating a suitable cybersecurity architecture. After a comprehensive and iterative literature search, several cybersecurity architectures were identified (Table 2). Most of the cybersecurity architectures were developed by cybersecurity organizations based on reports and white papers from consulting firms and international organizations. The cybersecurity architectures identified have been published within the last ten years, from 2013 to 2023, and are based on different perspectives.

4. Proposed Cybersecurity Architecture

Cybersecurity solutions should address each step with a targeted solution while maintaining an overall focus on security. Having a general sense of cybersecurity framework is no longer enough. An intricate network of security measures, layered atop one another, consolidates cybersecurity domains. Cybersecurity domains is a term used to describe different areas where cybersecurity practices can be applied. Each aspect of the cyber domain presents unique security challenges and risks that require attention. To ensure cybersecurity,

organizations must identify and mitigate risks associated with every subdomain. This holistic view of organizational information security allows cybersecurity specialists to apply different approaches to different parts of cyber domains.

4.1 Proposed Cybersecurity Architectures

A coordinated effort is vital in maintaining a good cyber security posture as organizational assets are comprised of various platforms. The web of cybersecurity measures working together to protect a system is called cybersecurity domains.

The proposed cybersecurity architecture makes use of the NIST framework (Identify, Protect, Detect, Respond, Recover) "GOALS" as the foundation (these are further discussed in Section 5.1) and utilises the pillars from the CIA triad (Confidentiality, Integrity, Authenticity) at the CENTER (discussed in Section 5.2) and finally offer nine (9) subdomains as the core of the architecture (discussed in Section 5.3).

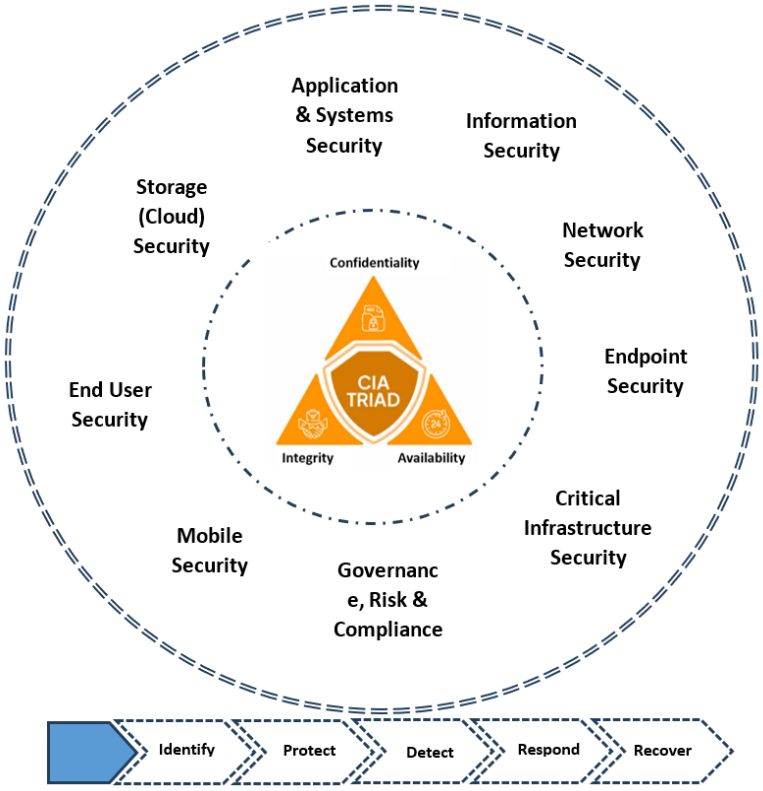

Figure 1: Proposed Comprehensive Cybersecurity Architecture

The proposed cybersecurity architecture can be refined over time to ensure it is comprehensive and covers every angle /inch of an organization.

5. Discussion on Proposed Cybersecurity Architecture

This section discusses the proposed cybersecurity architecture, motivating each component making the architecture. This section discusses the five NIST functions, followed by the CIA Triad, and finally the nine (9) cybersecurity domains.

5.1 NIST Goals

The National Institute of Standards and Technology (NIST) is a worldwide recognised information security best practice framework (Almuhammadi & Alsaleh, 2017). The NIST Information Security Framework consists of a collection of industry standards and best practices. The NIST framework comprises of five functions that operate concurrently and continuously (Möller, 2023; Malatji, Marnewick & Von Solms, 2022). When implemented together, these functions provide a comprehensive and strategic view of the cybersecurity risk management program (Curtis & Mehravari, 2015, Le & Hoang, 2017). The NIST information security framework offers the following five (5) different functions/goals:

- IDENTIFY**:** refers to tools to track and trace every IT asset running within an organization (Almuhammadi & Alsaleh, 2017)
- PROTECT**:** refers to tools used to protect all identified assets (Sulistyowati, Handayani & Suryanto, 2020)
- DETECT**:** refers to tools for monitoring the organisation and detecting intruders (Möller, 2023)
- RESPOND**:** refers to automated tools that flag incidents and direct ticket assignments accordingly (Le & Hoang, 2017)
- RECOVER**:** refers to rapid recovery to normal functionality after a cyberattack (Curtis & Mehravari, 2015)

5.2 CIA Triad

Also known as the pillars of information security, the CIA triad comprises of Confidentiality, Integrity and Availability. The terms 'confidentiality', 'integrity' and 'availability' have been widely used in the information security practice and in academic literature to help evaluate and create information systems (Qadir & Quadri , 2016; Fenrich, 2008). CIA triad still continues to assume a major role in information security practice as they offer the fundamental elements of security controls in information systems (Samonas & Coss, 2014). Essentially, this means that a sound information security system must protect confidentiality, integrity, and availability. The CIA triad has not only shaped and informed the theoretical understanding of information security, but also the very practices through which security is developed and implemented in organizations (Hiza, 2022). Following are definitions of each pillar of information security:

- CONFIDENTIALITY**:** this refers to the protection of information from unauthorized or unintended disclosure (Lundgre n & Möller, 2019; Fenrich, 2008)
- INTEGRITY**:** this refers to the prevention of unauthorized information alteration or destruction (Hiza, 2022; Samonas & Coss, 2014)
- AVAILABILITY**:** this refers to judicious and reliable access and use of data and information, whenever and wherever it is needed by the appropriate parties (Qadir & Quadri, 2016; Hiza, 2022)

5.3 Cybersecurity Domains

The last component of the proposed cybersecurity architecture are the nine (9) cybersecurity domains. Each domain should satisfy confidentiality, integrity and availability, as well as the five NIST goals (identify, protect, detect, respond and recover). The following section discusses the nine cybersecurity domains:

APPLICATION AND SYSTEM SECURITY**:** involves creating, adding, and testing security features in applications to prevent cyber-attacks and make them secure. Ensures security of existing software and applications and defends against threats during the application's development stage. This allows organisations to install many layers of security within a software and to any information related to it, also limit unwanted changes to the software information (Usman, Jan, He & Chen, 2019; Sabillon, Serra-Ruiz, Cavaller and Cano, 2017).

INFORMATION SECURITY**:** this domain protects all kinds of data from unauthorized access and prevents any changes, modifications, disclosures, and deletions. It protects sensitive business information and ensures data security (Obrst, Chase & Markeloff, 2012).

NETWORK SECURITY**:** this involves protecting computer networks and network-accessible resources from unauthorized access and modifications. Network security combines strategies, technologies, and processes that protect a network from intrusion (Sabillon, Serra-Ruiz, Cavaller and Cano, 2017; Usman, Jan, He & Chen, 2019).

ENDPOINT SECURITY: the protection of end-user devices such as desktops, laptops, mobile phones, and tablets from malicious threats and cyberattacks. This includes scanning all the devices from a network for threats, anomalies, and suspicious behaviour (Wang, Lau & Gerdes, 2018; Obrst, Chase & Markeloff, 2012).

CRITICAL INFRASTRUCTURE SECURITY**:** refers to protecting the infrastructure without which the security of a nation may be in danger. It consists of both cyber and physical systems crucial to ensuring cyber security. The cybersecurity of any organization can run smoothly when the physical assets of the company are safeguarded (Collier, Linkov & Lambert, 2013).

GOVERNANCE, RISK & COMPLIANCE**:** refers to the development and creation of company policies on various aspects of internal and external security. The strategy of any organization to deal with potential and real cyber

security attacks. This includes the development of preventive and recovery systems to manage and respond to potential cyber threats (Usman, Jan, He & Chen, 2019; Obrst, Chase & Markeloff, 2012).

MOBILE SECURITY**:** protects mobile devices or tablets from any malicious threats of data loss or asset loss. With the popularity of mobile, it has become an essential part of cybersecurity (Sabillon, Serra-Ruiz, Cavaller and Cano, 2017).

END-USER SECURITY**:** training employees and people on cybercrimes, and industry best practices and protecting themselves from threats like social engineering are incredibly important. This will either prevent unnecessary attacks or enable individuals to identify risks themselves (Wang, Lau & Gerdes, 2018).

CLOUD SECURITY**:** protects the cloud infrastructure, environment, applications, and data from threats. It ensures the authentication of end users and devices and provides data privacy protection (Wang, Lau & Gerdes, 2018; Obrst, Chase & Markeloff, 2012).

5.4 Benefits of Proposed Cybersecurity Architecture

Security professionals must present cybersecurity data in a way that satisfies executives' curiosity, leads to actionable insights, and is easy to understand. The benefits of the proposed cybersecurity architecture include:

- *A comprehensive cybersecurity structure:* the proposed cybersecurity architecture is an amalgamation of numerous cybersecurity frameworks merging their strengths and benefits.
- *Offers a bird's eye view of the organisation:* the proposed cybersecurity architecture allows one to work on multiple plains of cyberattacks, all at once.
- *Offers better control over the environment:* the proposed cybersecurity architecture allows one to determine risk tolerance and set controls.
- *Contextualise cybersecurity solution:* Depending on the context and requirements of an environment, domains can be added or removed from the proposed cybersecurity architecture. However, some organizations are more advanced than others.

Security professionals need to carefully choose the most appropriate metrics while presenting reports to business teams. It is important to report the outcomes of cybersecurity solutions and their impact on organization's assets, operations, and reputation. A combination of quantitative and qualitative measures can be used, such as key performance indicators (KPIs), key risk indicators (KRIs), return on investment (ROI), cost of risk (COR), customer satisfaction, and stakeholder feedback.

The ability to quickly learn from failures, adapt and repurpose is critical to successfully measure cybersecurity.

6. Conclusion

The recent high-profile security breaches of organizations have demonstrated the need for good cybersecurity measures. These breaches have resulted in the loss of incredibly sensitive user information, causing irreversible financial and reputational damage. Every day, attackers target companies of all sizes to steal sensitive information or disrupt operations. Companies are often unaware of the many threats that exist within their IT infrastructure, and as a result, they do not implement cyber security countermeasures until it is much too late. In the near future, it is unlikely that the frequency or intensity of cyberattacks will decrease. Attacks on critical infrastructure are expected to increase in both strength and sophistication over time. The aim of the study was twofold: first, it provides an in-depth review of cybersecurity architectures; second, it proposes a cybersecurity architecture that extends existing cybersecurity architectures. The in-depth review features five most popular and widely used cybersecurity frameworks. The proposed cybersecurity architecture has the NIST goals as a foundation and the CIA triad at the center. The proposed cybersecurity architecture has domains such as application and Systems security, Information security, Network security, End-point security, Critical Infrastructure security, Mobile security, Storage security etc. The proposed cybersecurity architecture seeks to assist cybersecurity consultants in answering questions from executives such as: Are we secure? Are security investments delivering value to the business? What is our preparedness for a cyberattack? The benefits of the proposed cybersecurity architecture include a comprehensive cybersecurity architecture; offers a bird's eye view of the organisations' security posture; offer better control of the environment and an architecture that can be tailored to meet organisational needs and requirements.

References

Almuhammadi, S., and Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. Computer Science & Information Technology (CS & IT), 7(3), 51-62.

Aphane, M. P. (2023). Cybersecurity Awareness on Cybercrime Among the Youth in Gauteng Province. International Journal of Social Science Research and Review, 6(8), 23-32.

Bhattacharyya, D. K. (2009). Research methodology. Excel Books India.

Carcary, M., Doherty, E., and Conway, G. (2019). A framework for managing cybersecurity effectiveness in the digital context. In European Conference on Cyber Warfare and Security (pp. 78-86). Academic Conferences International Limited.

Collier, Z. A., Linkov, I., and Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. Environment Systems and Decisions, 33, 469-470.

Curtis, P. D., and Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. In 2015 IEEE international symposium on technologies for homeland security (hst) (pp. 1-6). IEEE.

Fenrich, K. (2008). Securing your control system: the" CIA triad" is a widely used benchmark for evaluating information system security effectiveness. Power Engineering, 112(2), 44-49.

Fowler, S., and Chen, P. P. (2017). CsPI: A New Way to Evaluate Cybersecurity Investments: A Position Paper. In 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 283-284). IEEE.

Goddard, W., and Melville, S. (2004). Research methodology: An introduction. Juta and Company Ltd.

Hallman, R. A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., Slayback, S. M., and San Miguel, J. M. (2021). Determining a return on investment for cybersecurity technologies in networked critical infrastructures. International Journal of Organizational and Collective Intelligence (IJOCI), 11(2), 91-112.

Hallman, R. A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., John, M., and Miguel, S. (2020). Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value That Cybersecurity Technologies Provide after Integration. In COMPLEXIS (pp. 43-52).

HIZA, D. (2022). Assessing the Significance of Cia Triad Security Model in Establishing ICT Security Controls in The Public Sector (Doctoral dissertation, Institute of Accountancy Arusha (IAA)).

Ivanov, D. and Das, A. (2020). 'Coronavirus (COVID-19/SARS-CoV-2) and supply chain resilience: A research note', International Journal of Integrated Supply Management 13(1), 90–102. https://doi.org/10.1504/IJISM.2020.107780

Ivanov, D. and Dolgui, A. (2021). 'A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0', Production Planning & Control 32(9), 775–788. https://doi.org/10.1080/09537287.2020.1768450

Le, N. T., and Hoang, D. B. (2017). Capability maturity model and metrics framework for cyber cloud security. Scalable Computing.

Lundgren, B., and Möller, N. (2019). Defining information security. Science and engineering ethics, 25, 419-441.

Malatji, M., Marnewick, A. L., and Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security, 30(2), 255-279.

Mbelli, T. M., and Dwolatzky, B. (2016). Cyber security, a threat to cyber banking in South Africa: An approach to network and application security. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 1-6). IEEE.

Möller, D. P. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 231-271). Cham: Springer Nature Switzerland.

Moore, T., Dynes, S., and Chang, F. R. (2016). Identifying how firms manage cybersecurity investment. In Workshop on the Economics of Information Security (WEIS) (pp. 1-27).

Obrst, L., Chase, P., and Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. In STIDS (pp. 49-56).

PwC (2018). Navigating the rising tide of uncertainty, 23rd Annual Global CEO Survey. Accessed 09 November 2023 at https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2020.html

Qadir, S., and Quadri, S. M. K. (2016). Information availability: An insight into the most important attribute of information security. Journal of Information Security, 7(3), 185-194.

Rajasekar, D., and Verma, R. (2013). Research methodology. Archers & Elevators Publishing House.

Roy, A., Kim, D. S., and Trivedi, K. S. (2010). Cyber security analysis using attack countermeasure trees. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (pp. 1-4).

Sabillon, R., Serra-Ruiz, J., Cavaller, V., and Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In 2017 International Conference on Information Systems and Computer Science (INCISCOS) (pp. 253-259). IEEE.

Samonas, S., and Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3).

Singh, S., and Kumar, S. (2020). The times of cyber attacks. Acta Technica Corviniensis-Bulletin of Engineering, 13(3), 133-137.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333-339.

Sulistyowati, D., Handayani, F., and Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV: International Journal on Informatics Visualization, 4(4), 225-230.

Usman, M., Jan, M. A., He, X., and Chen, J. (2019). A survey on representation learning efforts in cybersecurity domain. ACM Computing Surveys (CSUR), 52(6), 1-28.

Wang, H., Lau, N., and Gerdes, R. M. (2018). Examining cybersecurity of cyberphysical systems for critical infrastructures through work domain analysis. Human factors, 60(5), 699-718.

World Economic Forum (WEF). (2017). Impact of the Fourth Industrial Revolution on supply chains, System Initiative on Shaping the Future of Production, World Economic Forum, Geneva.

World Trade Organisation (WTO). (2020). E-commerce, trade and the Covid-19 pandemic, pp. 1–8, WTO Secretariat, Geneva.