Mitigating Cybercrimes in An Evolving Organizational Landscape

Abel Yeboah-Ofori[1]*
School of Computing and Engineering, University of West London, London, UK
Abel.yeboah-ofori@wwl.ac.uk
Francisca Afua Opoku-Boateng[2]
Department of Computer Science, California State University, Fullerton, USA
fopokuboateng@fullerton.edu

Abstract
Purpose – Various organizational landscape has evolved to improve their business processes, increase production speed and reduce the cost of distribution, and has integrated their internet with SMEs and third-party vendors to improve business growth and increase global market share, including changing organizational requirements and business process collaborations. Benefits include a reduction in the cost of production, online services, online payments, product distribution channels, and delivery in a supply chain environment. However, the integration has led to an exponential increase in cybercrimes, with adversaries using various attack methods to penetrate and exploit the organizational network. Thus, identifying the attack vectors in the event of cyberattacks is very important in mitigating cybercrimes effectively and has become inevitable. However, the invincibility nature of cybercrimes makes it challenging to detect and predict the threat probabilities and the cascading impact in an evolving organization landscape leading to malware, ransomware, data theft, and denial of service attacks, among others. The paper explores the cybercrime threat landscape, considers the impact of the attacks, and identifies mitigating circumstances to improve security controls in an evolving organizational landscape.
Design/methodology/approach – The approach follows two main cybercrime framework design principles that focus on existing attack detection phases and propose a cyber crime mitigation framework that uses detect, assess, analyze, evaluate and respond phases and subphases to reduce the attack surface. The methods and implementation processes were derived by identifying an organizational goal, attack vectors, threat landscape, identification of attacks and models, and validation of framework standards to improve security. The novelty contribution of this paper is threefold: First, we explore the existing threat landscapes, various cybercrimes, models, and the methods that adversaries are deploying on organizations. Secondly, we propose a threat model required for mitigating the risk factors. Finally, we recommend control mechanisms in line with security standards to improve security.
Findings – The results show that cybercrimes can be mitigated using a cyber crime mitigation framework to detect, assess, analyze, evaluate and respond to cybercrimes to improve security in an evolving organizational threat landscape.
Research limitations/implications – The paper does not consider the organizational size between large organizations and SMEs. The challenges facing the evolving organizational threat landscape include vulnerabilities brought about by the integrations of various network nodes. Factor influencing these vulnerabilities includes inadequate threat intelligence gathering, a lack of third-party auditing, and inadequate control mechanisms leading to various manipulations, exploitations, exfiltration, and obfuscations.
Practical implications – Attack methods are applied to a case study for the implementation to evaluate the model based on the design principles. Inadequate cyber threat intelligence gathering, inadequate attack modelling, and security misconfigurations are some of the key factors leading to practical implications in mitigating cybercrimes.
Social implications – There are no social implications; however, cybercrimes have severe consequences for organizations and third-party vendors that integrate their network systems, leading to legal and reputational damage.
Originality/value – The paper's originality considers mitigating cybercrimes in an evolving organization landscape that requires strategic, tactical and operational management imperative using the proposed framework phases, including detect, assess, analyze, evaluate and respond phases and subphases to reduce the attack surface, which is currently inadequate.

Keywords: Cybercrime, Cyberattack, Mitigations, Cyber threat Landscape, Threat Modelling, Cybercrime Mitigation Framework,
Paper type - Research paper

1. Introduction

The cyberspace and internet provides organizations the capabilities to evolve and integrate their network system with other organizations and third-party vendors to transact online business locally and globally as it removes barriers and maximizes time to market in a cyber supply chain environment (Pawar and Palivela, 2022; Yeboah-Ofori et al. 2022). Further, the Covid-19 pandemic has heightened the need for increased dependency on the internet by organizations to facilitate their business processes and provide greater reach (Thomas and Sule, 2022). However, that led to various cyberattacks and disruption of services (Nabe 2021). Major organizations such as BA and Twitch have experienced cybercrimes that have led to data breaches, disruption of services, fines of £183m, reputational damage, and other issues such as resources spent in investigating and responding to the breaches as well as recovering and restoring the systems to normal usage after the attacks. For instance, British Airways experienced a data breach attack that led to about 500,000 customers' personal data being stolen, including credit card details, and the Twitch data breach attack that has led to the stolen of 125gb of sensitive customer and employee data being breached (Paul, 2021; The Economist, 2018). Internet growth and global market share have evolved to include business process collaborations, reduction in the cost of production, online services, online payments, product distribution, and delivery in a supply chain environment. Thus, countering threats from cyber and information risks could maximize cyber supply chain systems towards a more effective and holistic approach to risk management. Factors influencing the use of eCommerce platforms and evolving organizational landscape include global competition, global market expansion, increased market share, 24/7 online services availability of electronic products, cloud computing, use of mobile apps transactions, Bring Your Own Device (BYOD), home delivery, online sales, and purchases are some of the reasons why the organizational environment is evolving. Online marketing leverages on internet technology to provide services (Dwivedi et al., 2021). The Mobile and cloud environment has evolved, and so have the risk and controls (Camillo et al, 2012). Razzaq et al. (2014) highlight the challenges in conventional web applications detections techniques leading to various online attacks. Cyber supply chain systems integrate various organizational business requirements, processes, and information flows to provide services and products to meet organizational goals and customer needs (Yeboah-Ofori et al., 2019). These integrations may lead to cybercrimes, threats, risks, and vulnerability challenges in the event of an attack on one organization. Consequently, Hannibal et al. (2022) highlight the lack of universally accepted supply chain risk management and suggest the need to understand barriers to information sharing in managing the risk (Hannibal et al., 2022). To meet the changing business requirements and improve organizational processes and overall business continuity, various organizations have integrated their operational technologies with other organizations, small and medium scale enterprises (SMEs), and third-party vendors to improve business processes, increase production speed and reduce the cost of distribution (Yeboah-Ofori et al., 2019). The emergence of electronic transactions, third-party vendors, and online banking services have evolved over time and brought a lot of changes to how organizations and industries operate. Bissell et al., (2022) posit that 40% of security breaches are now indirect as threat actors target the weak links in the supply chain or business ecosystems (Bissell et al., 2022). Anderson et al., (2019) posit that measuring the changing cost of cybercrime has been challenging due to advancements in electronic banking and e-commerce including the use of new apps such as ride-hailing, cryptocurrency, and migration of data to a cloud environment leading to a variety of attacks (Anderson et al., 2019).

Further, various organizations no longer run their business on a single server but from distributed platforms using the internet to meet global product demands and business expansions. Furthermore, the integrated and distributed nature of organizational internet infrastructures with SMEs and third-party vendors has increased vulnerable spots and has led to experiences of various cyberattacks and cybercrime. Thus, considering a supply chain from risk mitigation through sharing information has become challenging (Hannibal et al., 2022). Additionally, inherent complexities in web application design and conventional detection techniques are struggling (Razzaq et al, 2014) due to the increased use of web applications, mobile devices and cloud computing by businesses, organizations and individuals are causing more threats, vulnerabilities and attacks to sensitive data such as identity theft, intellectual property theft and financial fraud. The cybercrime threat landscape is also evolving due to the changing cyber threat landscape, changing laws and legislations and lack of cyber security expertise (Gercke, 2012: Zappa, 2014). Factors such as changes in service delivery, changes in distribution supply chain channels, evolving organizational requirement, business trends, and their global nature have given most organizations the impetus to evolve to meet global economic demands and business expansions. Moreover, financial institutions and bank transactions have evolved to include electronic banking, electronic products, and services available anytime and anywhere, product time to advertise, market service imperatives, and online financial services. Consequently, these new trends in electronic products and services that the banking industries are using have also brought about a lot of vulnerabilities, threats, and attacks to extraordinary levels. Thus, mitigating cybercrimes could provide a cyber resilience environment for organizations to understand the threat landscape and gain situational awareness in the supply chain environment to ensure business continuity (Yeboah-Ofori et al., 2022). For instance, Camillo et al. (2012) posit that evolving organizational requirements and varying organizational business process requirements, and the continued adoption of web applications, mobile, cloud, and social media technologies to facilitate business processes have in recent times, increased opportunities for attackers in terms of online purchases, payments using card payments (Camillo et al., 2012). The fact that most organizations are also collaborating with various banks to complete transactions online has contributed hugely to cybercrime threats, vulnerabilities, and attacks. Cybercrime is the ultimate threat to all organizations across the globe and one of the most significant problems with human aspect (Morgan, S. (2019). As technology advances, cybercrimes have increased exponentially, with adversaries using various Advanced Persistent Threats (APT) methods to penetrate and exploit the organizational threat landscapes. Cybercrimes are coordinated by individuals or groups (Kaspersky, (2021). Cybercrimes are criminal activities such as cyber fraud and theft committed using computers and the internet to illegally access, transmit or distribute data (Mokha, 2017; Yeboah-Ofori and Islam, 2019). These illegal activities can cause severe damage, such as social psychological, physical, or financial loss to individual users and organizations (Mokha, 2017). Several reasons lead to cybercrimes which are additionally dominant. These reasons could range from easy and cheap mobile phone or IoT device access to internet access (Sattar, 2018). OWASP ASVS, (2021) application security verification standards outline the various web application changing trends and how the attacks are impacting organizations. The trends represent a broad consensus on now web application risks and their criticality (OWASP ASVS, 2021). Unfortunately, the hard truth is that several organizations are still unaware of the effects of internet usage and have become victims of cybercrimes (Sattar, 2018).

The paper does not consider the organizational size between large organizations and SMEs. It focused on integrating organizational network systems with SMEs and third-party vendors in a supply chain environment for business processes and how cybercrimes can be deployed on an SME to gain access to a large organization. A start-up organization is the most vulnerable. Thus, not asking a start-up organization to comply with so many standards and follow rigorous risk assessment processes is very dangerous and detrimental to any major organization that wants to evolve, survive and expand. Consider the impact of an Island-hopping attack or a watering hole attack on the start-up organization and the financial, reputation, and legal implications it may have on the organization. Consider the cost of alternatives for not ensuring compliance. An Island-hopping attack is a hacking technique in which threat actors target an organization's vulnerable third-party partners to undermine the organization's security defence and gain access to their network (TechTarget Contributor 2020). The challenges facing the evolving organizational threat landscape include vulnerabilities brought about by the integrations of various network nodes. Factor influencing these vulnerabilities includes inadequate threat intelligence gathering, a lack of third-party auditing, and inadequate control mechanisms leading to various penetrations, manipulations, exploitations, exfiltration, and obfuscations. Thus, it is essential to mitigate cybercrimes on all the integrated networks to ensure parallel security.

1.1 Recent Cybercrime Cases

Cyberattacks and cybercrimes have increased exponentially, and their impact on evolving organizations has extended in the size of organizations, the complexity of the integrated networks, and the cost of impact (Morgan, 2019; Summerville, 2017). Recently, several cybercrime incidents with severe consequences have been highlighted that have targeted and crippled many high-profile organizations and companies (Touro, 2021). For instance, a ransomware attack on the colonial pipeline company affected the company's billing systems and network (Summerville, 2017). Twitch, a parent gaming company of Amazon, experienced a major breach that led to the attackers stealing 125gibabites of most sensitive customer and employees data. The attackers used phishing campaigns to obtain employee credentials, and gain access to sensitive data (Paul, 2021).

That led to a pervasive lack of gasoline in several states and significantly impacted consumers, causing fear and panic. Notably, the pipeline is essential to the national critical infrastructure system. Similarly, JBS Foods, the world's largest meat packing company, ended up paying a demanded ransom of $11 million after the cyberattack (Reuters, 2021). Other high-profile cyberattacks on organizations and victims include the Steamship Authority of Massachusetts, which impacted the ferry services (NDC News, 2021), the University of California Schools (Morgan, 2021), and the Washington DC Metropolitan Police Department (Brewster, 2021).

Cyberthreats targeting organizations have increased with the latest cybercrime reported in 2021 by finance online review businesses, leading to various manipulation, exfiltration, and obfuscation (FinanceOnline, 2019). The cybercrime trends as listed from the highest to lowest, including Malware, phishing, ransomware, account takeover, DoS, web application attacks, Advance persistent threats, insider threats, and zero-day attacks. Organizations impersonated by phishing attacks identify the leading organization prone to impersonation attacks through phishing attacks, with Microsoft corporation being the leading organization that is most targeted and PayPay being the least targeted organization. Leading cyber threat hunting inhibitors identifies some of the challenges facing leading cyber threat hunting, including the difficulty of implementing hunting technologies as the highest, lack of skilled personnel, lack of budget, lack of solutions, and the lack of third-party validations of threat hunting tools as the least (FinanceOnline, 2019).

1.2 Impart Cybercrime on Organizations

The global impact of cybercrime in the event of attacks leads to financial loss, reputational damage, disruption of services, and litigation issues for organizations. Cybercriminals are exploiting security weaknesses and causing data breaches in companies, governments, and healthcare organizations, sometimes demanding millions of dollars in payment (Touro, 2020). Saudi Aramco's electric power grid experienced a cyberattack in 2017, where the system was shut down, leading to disruptions of services to major organizations. Ukraine Power Grid attack in 2015 led to a blackout in the whole country for hours, and it impacted greatly on the countries critical infrastructure supply chains systems (Zetter, 2016). The Auditor General of the Department of Health (2017) reported a Wannacry Ransomware attack that affected the NHS and over 200,000 computers in about 100 countries. The attack led to major incidents and disrupted services on the NHS emergency services, patient health, and patient care records (Auditor General of the Department of Health 2017). A cybersecurity 2020 reports that the impact of cybercrimes has increased, and the cost of damage and destruction of service, data, loss of productivity, and theft of intellectual property, among others, from cybercrimes per second was $190,000 with an annual damage cost of 6 trillion dollars (Morgan, 2019). A Ransomware cyberattack on the JBS food chain led to a disruption of services, data deletion, and reputational damages to its other companies in Brazil, Canada, the USA, and Australia. The JSB food chain paid a ransom of paid $11 million to the attackers before the system was restored (Reuters, 2021). These recent cyberattacks have led attackers to exploit vectors, which ultimately results in the shutdown of critical infrastructures. Identifying the attack vectors in the event of cyberattacks is crucial in mitigating cybercrimes effectively. However, in the cybersecurity domain, the dynamic nature of cybercrimes makes it difficult and challenging to detect and predict the threat probabilities and the cascading impact of cybercrimes in an evolving organization landscape (Morgan, 2020). Further, cybercrime happens through advanced communication devices utilizing internet connections, which is challenging to detect the crime and identify the offenders (Ahmed, 2018).

According to the 2021 Data Breach Investigation Report, ransomware played a significantly increased role in Malware associated breaches of about 61.2% concerning previous years (Verison, 2021). ComPriTech, in one of their studies, shares how ransomware cyberattacks had a significant financial impact on the healthcare sector, with over 60% increase since 2019 and approximately $30 billion as an estimated cost for the attacks, which affected revenue, lawsuits, and ransom paid (Bischoff, 2020).

Existing frameworks provide standards, guidelines, and practices for cyberattacks and cybercrime mitigation and controls. For instance, NIST Framework for Improving Critical Infrastructure Cybersecurity (2018) provides common taxonomy and mechanisms for organizations (NIST 2018). MITRE (2013) Supply chain attack Framework and attack Patterns that provide a comprehensive set of data sources for and holistic view of supply chain attacks of malicious insertions and generate a catalog of attack patterns for cross-cutting needs (MITRE 2013). Thomas and Sule. (2022) propose a conceptual cybersecurity service system model that can provide a holistic, adaptive, and end-to-end view of the security approach. Leyden (2017) proposed a framework built around ISO/IEC29147-2014 standards. (Anderson, 2012) recommended a framework analyzing the cost of cybercrime. NIST SP 800-16 (2022) provides a cyber security supply chain risk management framework for managing risk through a supply chain system (Leyden, 2017). Razzaq et al. (2014) proposed a methodology to approach web application security that adopts the OWASP Mobile Application Security, among others (Razzaq et al., 2014). However, mitigating cybercrimes, risk and vulnerabilities are challenging due to the dynamic and changing nature of the threat landscape. Thus, cyber defence mechanisms do not provide absolute security to an organizational system. No organization can operate in cyberspace as an entity. Most organizations are integrated into a supply chain systems environment as part of their evolving nature. Thus, requiring cyber resilience and cybercrime mitigation techniques to ensure business continuity. For instance, Yeboah-Ofori et al. (2022) proposed a cyber resilience approach focusing on common critical assets using ML techniques and threat prediction to reduce the attack surface. The paper does not consider evolving organizations as an entity but rather from an integrated and supply chain system perspective. The paper addresses the cybercrime threat landscape, impact, and mitigation approaches from an integrated and evolving organizational landscape. For instance, threat actors are deploying island-hopping attacks on SMEs and third-party vendors using remote access trojan attacks to gain access to the small organizations or the SME’s network and then exploit the major organizations.

The papers explore the cybercrime threat landscape, considers its impact on evolving organizations, and identify mitigating circumstances to improve cybersecurity controls in an evolving organizational landscape. The objective of the paper is to discuss some of the cybercrime challenges impacting evolving organizations, compare existing frameworks, and propose a specific model to mitigate cybercrime in an evolving and integrated organization. The paper does not focus on an organization as a stand-alone rather, it considers organizations that have integrated their network with other organizations and third-party vendors.

The novelty contribution of this paper is threefold: First, we explore the evolving organizational landscape and how it integrates its network with SMEs and third-party vendors to improve business processes, cybercrime threat landscapes, existing security models, and the methods that adversaries are deploying on organizations. Secondly, we review some of the existing models and propose a model required for mitigating cybercrime. Finally, we recommend control mechanisms in line with security standards to improve security. The results show that cybercrimes can be mitigated using a cybercrime mitigation framework to detect, assess, analyze, evaluate and respond to cybercrimes to improve organizational security.

2. Related Works

This section discusses the related works and the state-of-the-art in cybercrime trends in evolving organizational landscape, the changing threat landscape, and some existing security frameworks used to mitigate cybercrimes. The Bank of England (2016) recommend the need to gather cyber threat intelligence (CTI) from organizations to understand cyberspace to be able to mitigate cybercrimes (Bank of Ghana 2016). Further, the evolving and integrating nature of the organizational business processes with SMEs and Third-party vendors requires that the existing security standards and policies be reviewed in line with the changing threat landscape. For instance, Fonseca-Herrera et al. (2021) postulate that the risks and threats to information security frequently affect the confidentiality, availability, and integrity of the company’s assets leading to physical, digital, economic, legal, psychological, social, and reputational damages. SMEs and other organizations play a significant role economically as they employ their workforce from society and use the internet to run their businesses. It is estimated that SMEs make up 99% of all businesses in the EU, employing 86.8 million people, equivalent to 66% of the workforce Zappa (2014). However, as they depend daily on the internet to facilitate their work process, these businesses are the most vulnerable and are victimized when it comes to cybercrimes. Cybercrimes and attacks have increased exponentially, leading to significant breaches and financial loss, disruptions, and reputational damages in most organizations Morgan, (2020). Considering how cybercrimes have emerged as a serious threat, it has been evident how worldwide governments, police departments, and intelligence units have all begun to react. Dashora, (2011) provided a glimpse into cybercrime in society, basing their research on several news media reports and portals (Dashora, 2011). Sattar et al., (2018) investigated the need to eliminate cybercrime hazards as this was becoming more critical. Their work focused on subjects either part of victimization by cybercrimes (Sattar et al., 2018). Ahmed et al. (2018) proposed a framework for automatic and manual techniques to detect cybercrime and charge the offender with proof (Ahmed et al. 2018). Furthermore, Bissell et al. (2022) explored what ultimately sets cybersecurity leaders apart in aiding and combating cybercrimes. The findings aimed at helping organizations innovate securely and build cyber resilience to assist in business growth with confidence (Bissell et al., 2022). However, cybercrime trends are increasing, leading to litigation issues, reputational damages, business shutdowns, and job losses. Regarding legal issues, Gercke, (2012) considered the evolving risk and controls in the cybercrime environment and proposed a global cybersecurity agenda, strategies, and solutions to the threat of cybercrime, especially for developing economies. The author posits that the risk associated with weak protection measures could affect developing nations more extremely. The Global Cybersecurity Agenda has seven main strategic goals, built on five areas: 1) legal measures; 2) Technical and Procedural Measures; 3) Organizational Structures; 4) Capacity Building; and 5) International Cooperation. The study theorizes that developing countries need to integrate protection measures into the roll-out of the internet, though this might raise the cost of the internet. However, developing cybercrime protection and technical measures to mitigate risk and promote proper cybercrime legislation is essential for both developed and developing nations (Gercke, M. 2012). Moreover, recognizing developing nations as potential cyber criminals have become challenging, and bringing them together with developed and emerging countries under one legal umbrella has critical (Zappa (2014). Additionally, Dwivedi et al., (2021) outlined issues facing digital and social media marketing organizations including artificial intelligence, augmented reality, digital contented management, mobile marketing and advertisements, B2B marketing electronic word of mouth, and ethical challenges that are being used to control consumer behaviors positively and negatively. Thus, mitigating cybercrimes in an organizational environment has become imperative to ensure business growth, market expansion, supply chain security, trust in service delivery and information assurance.

2.1 Existing Cybersecurity Frameworks

There are existing cybersecurity frameworks, standards, and policies that various organizations have adopted to provide security controls. However, due to the evolving organizational business process and the evolving threat landscape, the existing frameworks need to be revised to provide security mechanisms to prevent cybercrime. The NIST (2018) Framework for improving critical infrastructure cyber security provides standards, guidelines, and best practices for organizations to manage the cyber, physical, and people dimensions of cybersecurity risks (NIST (2018). The framework is composed of three main parts that each reinforce the connection between business drivers and cybersecurity activities: the framework core, framework implementation ties, and the framework profiles. The framework core considers a set of activities in line with standards, guidelines, and practices, their desired outcomes, and applicable references that are common across critical infrastructure sectors. It considers five concurrent functions including identify, protect, detect, respond and recover to provide a high-level strategic view of cyber security risk management. However, the framework is broad and challenging in applicability, considering it has about five categories with ninety-eight subcategories and does not provide specific cybercrime mitigation. The framework implementation tiers provide a perspective on how organizational entities view cybersecurity risk and the procedures to handle that risk (NIST, 2018). The tiers depict an escalating degree of consistency and complexity in managing risk practices. The implementation ranges from *Partial* Tier 1, reflecting a progression from formal information to *Adaptive* - Tier 4, a reactive response to the approaches that are agile and risk informed. The framework profiles represent outcomes of an organizational business requirements characterized by the various categories and based on the standards, guidelines, and practices aligned to the implementation scenario. The (NIST Cybersecurity Framework, 2018) has gained popularity and usage globally and with organizations as the implementation could be related to other standards such as ISO and COBIT, and ITIL to support systems development and cyber security controls (Chaphekar, 2019; Leal, 2016; Ozdemir; et al., 2014). However, the implementation ties, although useful, may not be usable in certain cybercrime incidents due to their generic profiles. Hitchcox, (2020) outlined some of the limitations of NIST cybersecurity frameworks that cybersecurity specialists must understand to reduce cybersecurity breaches by using a semi-structured approach to gather themes such as guidance to high-level outdated, limitations that negatively affect guidance implementation, lack of understanding of the importance of cyber security and compliance as not related to cybersecurity (Hitchcox, 2020).

Information Security Management Standards (ISMS) (ISO27002: 2017) provide a variety of security standards, guidelines, and procedures that can be implemented to ensure confidentiality, integrity, and availability of information for organizations. The ISO27000 framework provides a reference guide to how users can adopt the stages for their security implementation. Further, it defines specific control statements to satisfy the control objectives. However, the framework is broad and may only meet some organizational security requirements. COBIT provides a risk management framework that utilizes other sets of information technology controls to develop governance models appropriate for managing IT risk and auditing. The framework domains include organizational planning, acquisition, implementation delivery and support, monitoring and evaluation (Chaphekar, 2019). However, the framework is limited regarding the implementation tiers for business use, but it is more adopted by institutions. ITIL 4: (2019) is the latest version framework and provides a set of best practices and rules for IS service management with more agile support for digitizing the service processes (Leal. 2016). The framework consists of four functions, including guiding principles for service definitions, governance, service values, and service value chains that allow compliance and collaboration between the user, client, and suppliers (Ozdemir et al., 2014). However, the model relies on other frameworks, such as (ISO 27002 2017; NIST Cybersecurity Framework, 2018), to provide security standards and principles as it is not subject to security certification. Compared to COBIT, ITIL considers how its four functions and twenty-six processes are implemented, whiles COBIT determines what an organization needs to do (Chaphekar, 2019; Leal, 2016).

MITRE (2013) proposed a kill chain framework that describes the modelling of adversary behaviour used to compromise and operate within an organization's network. It enables a comprehensive evaluation of the network defence technologies, processes, and policies against adversary behaviours. MITRE Cyber Attack Lifecycle considers the tactics, techniques and procedures that describe an adversary model of the actions an adversary might take to compromise and operate within an enterprise network. It consists of seven phases: Reconnaissance, Weaponized, Deliver, Exploit, Control, Execute and Maintain. MITRE's 11 tactics and categories within ATT&CK for organizations were derived from the later stages (exploit, control, execute and maintain) of the seven stages Cyber Attack Lifecycle (MITRE (2013). However, the descriptions of the adversary's steps are generic and high level in applications across platforms and need to provide more technical details that are useful to specific attacks. Thomas and Sule. (2022) explore cyber security continuity and management for organizations subsistence and growth by proposing a holistic, proactive, and adaptive approach to cybersecurity from a services lens that considers cyberattacks, threats, and vulnerabilities from evolving organizational threat landscape. The authors considered the existing cybersecurity frameworks, standards, and best practices, including NIST Cybersecurity Framework, (2018) and ISMS, as well as the scope and implementation strategies at different levels of granularity. They proposed a dynamic end-to-end cybersecurity services model. The results show a proactive, adaptative and responsive model that could provide cybersecurity solutions (NIST Cybersecurity Framework, 2018). However, the model is generic and not specific to cybercrime or cyberattack incidents. Thus, its adaptive and responsive response to cybersecurity incidents will be applicably challenging. Razzaq et al. 2014) proposed an intelligent approach to web application security that could be used for ontological attack detection considering the increasing variety of online attacks. The authors demonstrated how an ontology-engineering methodology could be thoroughly applied to designing and evaluating security systems. More specifically, the proposed ontological model applied OWASP method to their work and how it captures the context and not the HTTP protocol specific attacks during request and response (Razzaq et al., 2014). A comprehensive metric for ontology evaluation was used to assess the proposed model's quality. The attack ontology model encompasses all the vulnerabilities mentioned in the OWASP top ten listed website attacks and shows improved performance and detection rate. However, the ontology engineering model is limited as it focuses on web application attacks on HTTP and does not consider HTTPS and how the attacks impact organizations. Other frameworks used in detecting cyberattacks have employed significant frameworks like the Open Web Application Security Project (OWASP), an online group that creates articles, methodologies, documentation, tools, and technologies in the area of web application security (Sucuri, 2021; OWASP, 2021). The OWASP top 10 is recognized worldwide by developers. The document highlights ten web application security risks and vulnerabilities to which organizations may be exposed. This risk includes Injection, broken authentication, and access control (OWASP, 2021). Yeboah and Brimicombe (2019) proposed mitigation techniques for cybercrime threats in social media using a systematic review process and a theoretical framework for cyber threat and open source intelligence. The proposed meta-analysis tool was utilized for the synthesis concepts from the literature reviewed and proposed an approach to mitigate cybercrime (Yeboah-Ofori, and Brimicombe, 2019). Furthermore, Mokha (2017) analyzed cybercrime awareness among internet users of different ages and educational qualifications. The authors identified a relationship between the respondents' age groups and educational qualifications; hence, individuals and all internet users owe themselves to be aware of cybercrime and security (Mokha, (2017). Nguyen (2020) examined what causes cybercrimes originating from Vietnam's social situation and ultimately highlighted the importance of the causes in cyberspaces (Nguyen, 2020). Back and LePrade (2019) recommended a more holistic approach using technology and a better understanding of the human factors that make cybercrime possible (Back and LePrade, 2019). Nadir and Bakhshi (2018) reviewed ransomware attacks' history and recent evolution. They ultimately provided a comprehensive taxonomic classification of the inherent attack vectors and currently available mitigation techniques (Nadir and Bakhshi, 2018). Yeboah-Ofori et al., (2019) proposed an approach to detect cybercrime and risks associated with a smart grid business application system to verify the motives and intents of the cybercriminal. Ultimately the authors identified business value, organizational requirements, threat agents, and impact vectors as four goals to mitigate the cybercrime risks (Yeboah-Ofori et al., 2019).

Leyden (2017) UK National Cyber Security Centre (NCSC) proposed a framework that is built around an established international standard for vulnerability disclosure, ISO/IEC29147-2014. The method aims to provide a faster and more efficient triage on reports of security flaws consistent with what NCSC describes as Active Cyber Defence. The framework identified and resolved vulnerabilities across three public-facing systems used in UK Public Sector organizations. However, the framework is generic and cannot be applied to any risk context. The model could be more conducive for evolving cybercrime threads, and the standard has been updated to ISO/IEC29147-2018 (Leyden, 2017). Anderson et al. (2012) considered the infrastructures supporting cybercrime and proposed a framework for analyzing the cost of cybercrime. A report requested by the Chief Scientist of the Ministry of Defence UK. The study looked at the cybercrime defence cost, direct losses and indirect losses, criminal revenue and cost to society. The report looked at the threats and the direct loss is the monetary equivalent of losses, damage or other suffering felt by the victim as a consequence of cybercrime. That is money withdrawn from the victim’s account, time and effort to reset account credentials, among others. That is money withdrawn from the victim’s account, time and effort to reset account credentials, and others. The indirect loss is the monetary equivalent of the losses and opportunity cost imposed on society by the cybercrime carried out and must be paid. The loss of trust in online banking, missed business opportunities, reduced uptakes by citizens, and effort to clean up. The defensive costs are the monetary equivalent of prevention efforts (Anderson et al., 2012). However, the framework needed further research, including insurance claims, litigation issues, and reputational damages. Fonseca-Herrera et al. (2021) presented a model for an information security management system based on the NTC-ISO/IEC 27001 standard that applies to an organizational information security requirement by implementing a systematic and adequate control mechanism, procedure and policies required to ensure CIA. The model allows the organization to define a security structure based on its business process, policies, and asset management to identify vulnerabilities and risks (Fonseca-Herrera et al., 2021). The model is relevant but needs to be revised as it did not consider the integrated and evolving nature of organizations and the changing threat landscape.

All the related works are relevant to contribute to the upturn of the knowledge for mitigating cybercrimes, among others. For instance, Thomas and Sule. (2022) proposed a holistic, proactive, and adaptive approach to cyberattacks, threats, and vulnerabilities, but it is not specific to any cybercrime incident and will be challenging when applied. NIST (2018) Framework for improving critical infrastructure security and provides standards, guidelines, and best practices. However, it is challenging in terms of applicability as it is broad and generic, with five categories and 98 subcategories. Razzaq et al. (2014) proposed a model for an intelligent approach to web application security using ontological-engineering methodology concepts for OWASP online attack detection (Razzaq et al., 2014). However, the model is limited to web application attacks on HTTP and does not consider HTTPS attacks. (MITRE, 2013) proposed a kill chain framework that describes the modelling of adversary behaviour, and the Attack Lifecycle considers the tactics, techniques, and procedures. However, the descriptions of the adversary's steps are generic and high level in applications across platforms. Yeboah-Ofori et al., (2019) proposed a model for mitigating cybercrime and risk for cyber physical systems by using Analytical Hierarchical Process (AHP) method to determine risk mitigation goals such as organizational business value, organizational requirements, threat agents and impact vectors (Yeboah-Ofori et al., 2019). The approach could have been more extensive in terms of applicability as it focused on systematic review only. (Anderson et al., 2012: Anderson et al., 2019) considered the infrastructures supporting cybercrime in the UK and proposed a framework for analyzing the cost of cybercrime, but it did not include litigation, insurance claims, and reputational damages for measuring the cost. Leyden (2017) proposed a framework built around an established international standard for vulnerability disclosure ISO/IEC29147-2014, but the model does not address the specific risk (Leyden, 2017). The existing works are relevant to current trends in the evolving organizational business process and cybercrime threats. However, they should have considered how to apply cybercrime mitigating framework strategies on an integrated and evolving organizational landscape to improve security. Our work focused on applying the proposed framework to a case study to mitigate cybercrimes.

3. Approach

The proposed approach considers the cybercrime mitigation phase that focuses on framework domains, phases, subphases, and standards for attack detection and mitigation. Our approach considers concepts from (NIST Framework, 2018; Razzaq et al., 2014; OWASP, 2021; MITRE, 2013; ISO27002, 2017) to develop and implement the proposed framework model. We derived the methods and implementation processes by identifying an organizational goal or actors, attack vectors, threat landscape, identification of attacks and models, and validation of framework standards and policies to improve security. Our work considers the framework mitigation concepts from an integrated and evolving organizational network and how an attacker can exploit the network to attack other organizations connected to a network. We did not consider it from an individual organizational perspective.

3.1 Identifying Cyber Crime Vectors

Identifying attack vectors in the event of cybercrime is crucial in effectively mitigating cybercrime. However, cybercrimes are unpredictable in the cyber security domain, making it difficult and challenging to predict the cyberattacks' threat probabilities and impacts. Although cybercrime, risks, and threats contain a lot of unpredictability, uncertainties, and fuzziness, cybercrime mitigation should be practical, systematic, and reasonable. Else it may not be applicable in the cyber security domain. Several methods have been deployed to mitigate cybercrimes. However, one of the ways to mitigate cybercrime is to integrate the modelling of attack vectors and subjective expert opinions to determine how threats propagate. We consider the following approach for our work. First, we identify all the organizational stakeholders and actors. These include the internal, external, and integrated system and all third-party vendors that have access to the organization's network infrastructure and may be complicit in any attack or unauthorized access. Further, we determine the attack vectors and vulnerable spots that could be exploited. These include the network nodes, access rights, privileges, passwords, firewalls, URLs, anti-virus, and authentication considered the threat landscape. Furthermore, the results of the threat landscape will assist in identifying the attacks and the proposed model. Finally, we identify the organizational assets, requirements, and business processes and may them against the proposed model. Secondly, after the development of the model, we consider the evaluation process, the standard, and the policies required to validate the model. Figure 1 depicts our approach as discussed

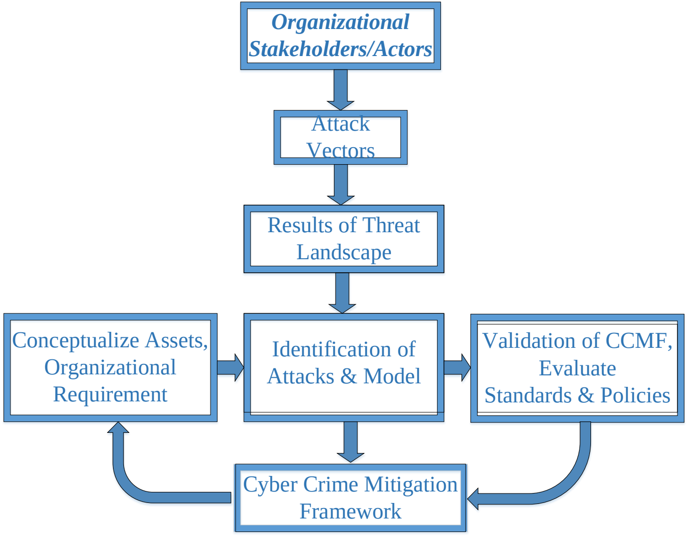
Organizational Stakeholders/Actors
Attack Vectors
Results of Threat Landscape
Conceptualize Assets, Organizational Requirement
Identification of Attacks & Model
Validation of CCMF, Evaluate Standards & Policies
Cyber Crime Mitigation Framework

Figure 1. Proposed Cybercrime Mitigation Approach

4. Implementation

This section provides a synopsis of the proposed approach and the processes in each phase of the proposed framework to mitigate cybercrimes. Note, our work considers the framework mitigation concepts from an integrated and evolving organizational network and how an attacker can exploit the network to attack other organizations connected to a network. We did not consider it from an individual organizational perspective.

4.1 Development of Proposed Framework

We utilize the (NIST 2018) framework concepts in designing the proposed framework. Further, we presented the Cyber Crime Mitigation Framework (CCMF) in line with the cybercrime threats and vulnerabilities identified in the introduction. In addition, we employ the JBS Food ransomware attack as a case study to identify organizational assets, attacks, and threats. Our results serve as input to the framework to identify the required elements to identify possible mitigation approaches.

4.1.1 Framework Principal

The CCMF offers a common language platform for the approach, guidance, concept, and implementation of cybercrime mitigation in an organizational environment. The phases in the framework provide a key set of uncomplicated requirements that will guide to achievement of the mitigation outcomes. These phases include (1) the framework domain, (2) Phases, (3) Sub phases, and (4) Standard references.

The principal phase comprises five phases- strategy management input and approvals required to achieve functional objectives. The five phases include: *Identity, Assess, Analyze, Evaluate and Respond*. Developing mitigation processes to thwart cybercrimes and their associated risks has been challenging in organizational space, development, and implementation. The challenges stem from the combination of key components identified in the organizational landscape, thus human factors, cyber digital, and cyber-physical systems. The strategic management committee must develop a security strategy for stakeholders within an organizational landscape to secure their systems from possible attacks. A security team will carry out the task of identifying, assessing, and reviewing cybercrime risk access spots of the system. The principal phases commit management to ensure cybercrime information is organized in a structured manner in line with the economy of the mechanism.

4.1.2 Concepts

The framework domains will align with organizational goals such as Business Value, Organizational requirements, Threat Agents, and Impact Vectors in line with standards, policies, processes, and technology. The nature of an organization's goal will determine the types of threats that can be initiated on the organization. These vulnerabilities can be exploited, and to an extent, the type of cybercrime attacks an organization may experience. Additionally, the framework can identify and cyber profile the organizational assets to focus on critical areas, as different organizations may have different threat levels. The Cyber Crime Mitigation Framework (CCMF) consists of Framework Phases, Sub Phases, a Standards Guide, and Framework Summary. The CCMF principal phases consider state-of-the-art reviews, frameworks, methodologies, and expert judgments. We follow the proposed CCMF process, as shown in Figure 2.

a) Framework Domain: Represents the organizational landscape areas such as Transport, Healthcare, Energy, Manufacturing, Finance, and Military. We seek to model the web application attack vectors between the organizational sectors' cross-domain security concerns for this research.

b) Phases: These are the principal phases that feed into the outcomes linked to the main organizational assets such as the Cyber-Physical Infrastructures, Cyber Digital coding structures, PLC, interfaces, and connectors, as well as the Human Elements such as the sensors and actuators.

c) Sub Phases: The subphase considers the implementation processes that stem from cybercrime categories that can be initiated by third parties such as suppliers, customers, external entities, intermediaries, and especially in a supply chain environment.

d) Standard Guides: involves set procedures in line with international standards. Policies and controls are to be applied when implementing the CCMF. Such as (NIST Cybersecurity Framework, 2018; OWASP ASVS, 2021; ISO 27002; NIST SP 800-161r1, 2022).

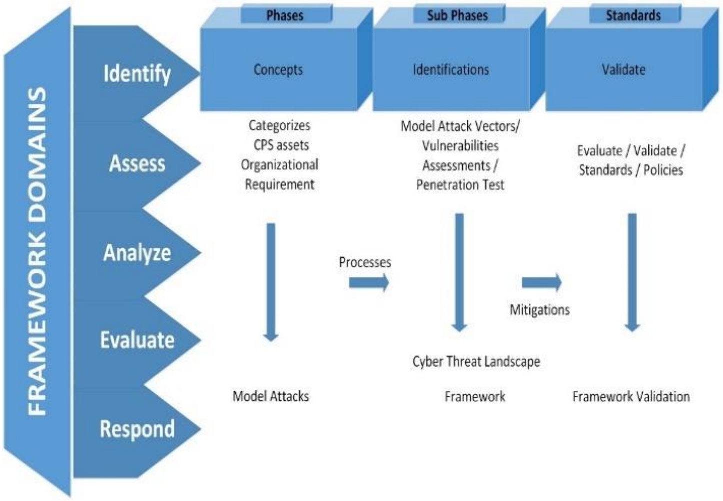

Figure 2. Proposal Cyber Crime Mitigation Framework Process

4.2 Cyber Crime Mitigation Framework (CCMF) Principal

The domain of the framework represents the organizational landscape and the associated systems. We develop a framework for mitigating cybercrime attacks on web applications in an organizational system for the paper. The implementation of the framework through an analysis and validation process follows the following steps. The purpose of listing numerous assessment methods and advocating various standards, regulations, and frameworks is to provide guidelines for security implementations for the validation of the framework as considered in Figure 2. The proposed framework automation process includes the following five phases: Identify, Assess, Analyze, Evaluate and Respond, as shown in Figure. 3. These phases are used to identify cybercrimes risks, threats, and vulnerabilities to put control parameters to prevent and respond to attacks.

4.3 CCMF Phases

The CCMF phases consist of five key components for the following risk mitigation processes required throughout the life of a business. These components include Identify. Assess, Analyze, Evaluate and Respond. We have discussed the phases in 4.3.1 to 4.3.5. Further, we have used a case study in 4.4 and the implementation phases from 4.4.1 to 4.4.5 as follows:

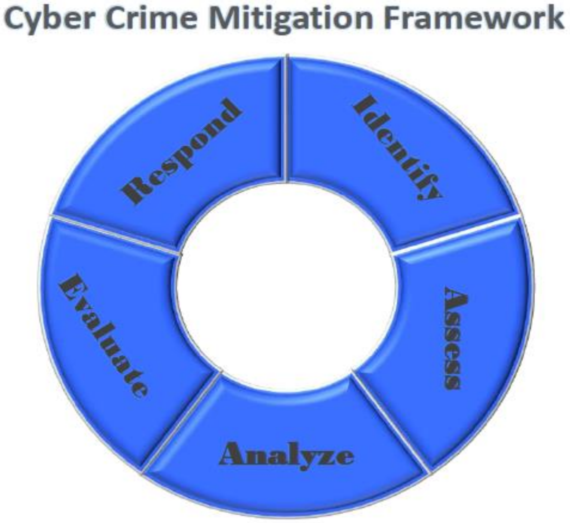

Figure 3 - Cyber Crime Mitigation Framework Phases

4.3.1 Phase 1- Identify

This phase includes identifying cybercrime areas where the stakeholders may have cross-cutting-domain concerns. For instance, the energy sector may connect its network nodes to the financial institution and the web application. We consider the external entities and the supplier chain environment, such as the customers, distributors, and suppliers. First, categorize all the assets in an organization. Then identify the probable internal and external threats, vulnerabilities, and cyber risk factors inherent in the system.

a) Sub Phase: As discussed in section C, this phase considers identifying the business process required to manage cyber risk in the interest of the organizational objectives, assets management, and business assurance throughout the organization's life. That includes the internal and external attacks initiated and vulnerabilities exploited by identifying all attacks determined by the output parameter, which then becomes the cybercrime attributes and the concepts. Based on the organization's business process and objectives, we may implement the vulnerability assessment or penetration test to determine the vulnerable spots on the system and the assets. These attacks could include hacking, SQL Injection, XSS attacks, and Broken Authentication.

*b) Standards**:*** We consider cybersecurity standards, regulations, best practices, expert judgments, and formal methods. The international standards include ISO27002 for ISMS, NIST Cyber Security Standard, and the OWASP Web Application Standards, such as the OWASP Proactive Controls 2018; OWASP ASVS, 2021; V5 Input Validation and Encoding. OWASP Testing: SQL, Command injection, OPRM Injections. OWASP Cheat Sheet: Injection Prevention. OWASP Cheat Sheet: SQL Injection Prevention.

4.3.2 Phase 2 - Assess

The assessment phase provides a proactive attempt to protect the system. That includes using the various cybercrime attacks on the system's vulnerable spots to identify threats such as supply chain compromises, ransomware or Malware, resonance, and Advance Persistent Threats (APT) attacks to assess vulnerabilities. For instance, an organization may select a particular event, such as a ransomware attack, perform a vulnerability assessment, and combine its probability with its potential impact. In addition, this phase includes risk assessments on the targeted profiles and attack modelling.

a) Sub Phase: We look at the attacks such as network penetrations, Injection flaws, and APT that may compromise the system. For instance, the adversary can penetrate, manipulate, and divert product delivery mechanisms before it gets to a final consumer using a supply chain compromise attack. We identify all the actors and access rights and privileges and carry out a risk assessment. This attack can occur at any stage of the supply chain and can impact data, software, or hardware.

b) Standards: The standards required here are National Supply Chain Risk Management Practices for Federal Information Systems. (NIST Cybersecurity Framework, 2018, OWASP ASVA, 2021; OWASP Proactive Controls 2018; IOS/IEC/IEEE 4210 System Architecture framework).

4.3.3 Phase 3 - Analyze

That includes investigating cyberattacks using digital forensics methods to systematically identify the cause of the cybercrime, how it happened, where it happened, and how it happened to determine the results.

a) Sub Phase: The digital forensics investigations method includes preserving the digital evidence and identifying if the attack requires live or dead analysis. Then, extracting evidence from digital media and analyzing the evidence to support or refute the hypothesis.

b) Standards: Includes Cybersecurity Enhance Act of 2014. BS EN OSO/IEC17020:2012, BS EN ISO/IEC17025, NIST Cybersecurity Framework, 2018.

4.3.4 Phase 4 - Evaluate

In this phase, we compare the state of a specific outcome of a cybercrime attack to the current state and the desired state. The results of the cyber risk assessment and the forensic investigations with a set of cyberattack criteria were listed in the identification phase to determine the business goals, risk tolerance, organizational resources, and the mitigation levels required. For instance, we assess the impact of XXS, SQL Injection, and CSRF attacks on current profiles.

a) Sub Phase: We may use SWOT analysis, Digital forensics results, and the attack models to reduce cyberattacks to organizational goals.

b) Standards: We consider the various standards, legal and regulatory requirements, and industry best practices, as well as compare the risk management priorities. BS EN ISO/IEC17020:2012, BS EN ISO/IEC17025, BS EN ISO/IEC17042, NIST Cybersecurity Framework, 2018.

4.3.5 Phase 5 - Respond

This phase seeks to develop measures to protect, mitigate and implement countermeasures to safeguard the organizational assets. These include Assess Controls, IT/IS Auditing, Backups, Data Security and Information protection, contingency planning, CERT, Policies, and Procedures in line with international standards.

a) Sub Phases: Training and workshops for staff, ensuring best practices, and certifying systems using recognized standard institutions.

b) Standards: OWASP ASVS, 2021; NIST Cybersecurity Framework (2018); ISO 27002; Cybersecurity Enhance Act of 2014. BS EN ISO/IEC17020:2012, BS EN ISO/IEC17025, NIST Cybersecurity Framework (2018).

4.4 Case Study

This section considers the JBS foods ransomware attack scenario as a case study for implementing the CCMF phases (Reuters, 2021). Our work focuses on how the attack occurred and how the proposed CCMF can be used to mitigate the attack. A ransomware attack was deployed on the JBS food company. The Brazilian meatpacker's arm in the United States and Pilgrims Pride Corp, a US chicken company owned mainly by JBS. The ransomware attack affected its supply chain service operations in Brazil, North America, and Australia. Additionally, the impact of the cyberattack made the subsidiary of the JBS company in Brazil halt their operations which threatened to disrupt food supply chains and further impacted food prices. A ransom was paid in bitcoins to the attackers. According to the report, a third-party company has been assigned to conduct a forensic investigation to establish how the incident occurred, and no final determination has been made. For further reading, we suggest you refer to (Reuters, 2021).

We used the case study to develop a threat model for our work The case study considers the CCMF phases to explain how the cyberattack was initiated and its cascading impacts. The attack phase considers the activities of how an adversary deploys an attack on the organization and the attack pattern used, including the vectors. The phase involves complex activities as all the stakeholders may have different system components, requirements, processes, and infrastructures. The purpose of listing numerous assessment methods and advocating various standards, regulations, and frameworks is to provide guidelines to security implementations for the validation of the framework as considered in Figure 2.

4.4.1 Phase One: Attack Pattern for Threat Modelling

Figure 4 discusses the attack pattern for the threat modelling for a cyberattack. We identify the nature of the attack pattern in the cybercrime domain where the stakeholders may have cross-cutting-domain concerns.

a) The adversary explores the organization's website, network system infrastructure, topologies, IP address, software, and configurations. That will inform the adversary of possible exploitations.

b) The adversary may use a botnet or rootkit attack to penetrate the network or deploy a phishing attack on a key staff member to penetrate the network when a malware-infected email. The email attaches itself to the person's address book and cascades to other networks, and infects the application process or shuts the system down, including other organizations connected to the network.

c) The attacker can deploy a remote Access Trojan (RAT) on the server and compromise the products, services, and delivery channels. Further, the attack can deploy a cross-site scripting attack on the organizational URL to penetrate and compromise the products.

d) Finally, the adversary can infiltrate and take command and control of the systems resources and cause many cybercrimes by manipulating the products, exfiltrating by stealing information, including intellectual property and industrial espionage attacks, and obfuscating changing their password regularly to maintain a presence.

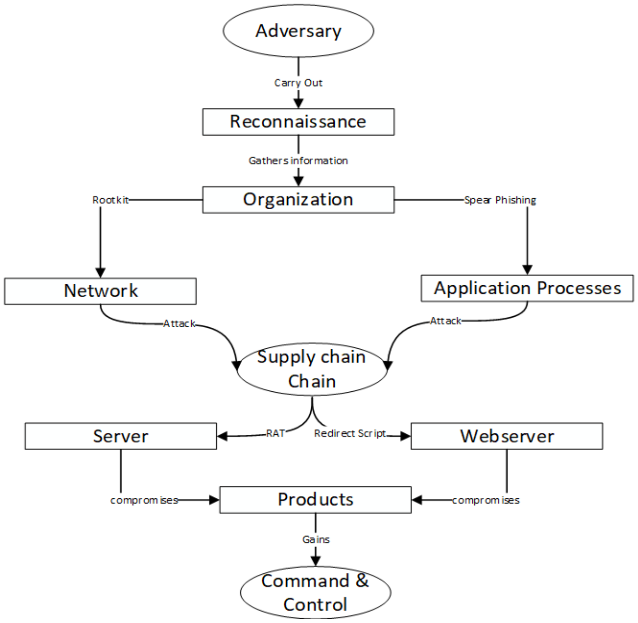

Figure. 4 - Threat Modelling for Cyberattack

This section discuss the our proposition the implementation process. Our work considers the framework mitigation concepts from an integrated and evolving organizational network and how an attacker can exploit the network to and the cascading impact of the attack to other organizations connected on a network. We did not consider it from an individual organizational perspective. The purpose of listing numerous assessment methods and advocating various standards, regulations, and frameworks is to provide guidelines to security implementations to support the framework implementation process discussed as follows.

4.4.2 Phase 2: Assess the attack was deployed

It provides a proactive attempt to ensure that the system is protected. That includes using the various cybercrime attacks on the system's vulnerable spots to identify threats such as compromises, ransomware or Malware, resonance, and Advance Persistent Threats (APT) attacks to assess vulnerabilities. The used Ransomware attack per the case study.

a) Identify what vulnerable spot on the system was exploited and how the ransomware attack was deployed: we determine what method was used to deploy the ransomware attack, such as a spear phishing attack to target the management staff who may be more vulnerable
b) The attacker gave a USB pen drive with the malware, botnet or rootkit virus to a staff who may not be aware of the vulnerability. When the victim inserts it, the attack propagates.
c) The impact is evaluated to determine how it affected the systems. We conduct a risk assessment by analyzing the risk using the Ransomware event, and evaluating the risks to determine the probability and impacts. For instance, a Likert scale of 1 to 5 and CVSS method to evaluate the impact. Further, we select the attack and combine the probability of it occurring with its cascading impact on the organization.
d) Treating the vulnerability: Implement security mechanisms such as authentications and authorization. Risk response strategies include risk transfer, risk avoidance, risk sharing, and reduction.
e) Review security policies in line with security mechanisms and risk monitoring.
f) Report assessments. That includes documenting the incident, vulnerabilities identified, causes of actions, response strategy and remediations.

4.4.3 Phase 3: Using Digital Forensic Investigation Process to Determine Attack

Investigates the cybercrimes using digital forensics methods to systematically identify the cause of the cybercrime, how it happened, where it happened, and how it happened to determine the results. This requires that we use the digital forensics incidence response and investigations process. We adopt the following in the digital forensics process:

We investigate the computers and the associated digital devices to determine how the incident occurred, who committed the crime, and how the attacker gained unauthorized access and deployed the activities.

a) Preservation: We preserve the state of the digital crime scene. The purpose of this phase is to reduce the amount of evidence that may need to be overwritten. The actions that are taken in this phase vary depending on the legal, business, or operational requirements of the investigation.

b) Identification: The identification processes can be used when investigating to determine the nature of crime both live and dead systems. A live analysis occurs when you use the operating system or other resources of the system being investigated to find evidence. A dead analysis occurs when you run a trusted application in a trusted operating system to find evidence. We used a dead analysis process as the incident has already occurred, and we are to investigate what happened.

c) Transport: the evidence is moved to the lab for further examination. The transport process includes preserving the state of the digital media when taking it to the lab for investigations after it has been identified as dead analysis. We take pictures to match them against the initial media to ensure a chain of custody. It also ensures that evidential integrity is maintained.

d) Acquisition or Extraction: we acquire or extract evidential data from digital media for examination. We use a write blocker tool to protect data from being written to before we carry out mirror images or copy the data for the analysis. The goal is to reduce the amount of evidence that can be overwritten during analysis.

e) Documentation of digital evidence: we document the digital evidence processes to ensure that there is continuity of evidence and chain of custody. It must be possible that we account for all that has happened to the exhibit between its original collection and its appearance in court preferably unaltered. It also ensures good record keeping. That includes the recorded date, time, questions asked, finding, and hypothesis.

f) Report Writing: We report the findings to clients. The report writing part of the digital forensic examination process is a very important link in the chain.

4.4.4 Phase 4: Evaluate the Impact of the Ransomware Attack

For our analysis, we compare the state of a specific outcome of a cybercrime attack to the current state and the desired state. The results of the analysis of the cyber threat intelligence gatherings, risk assessment, and forensic investigations using the CCMF provide us with a set of criteria listed in the identification phase to determine the business goals, risk tolerance, organizational resources, and mitigation levels required in line with Table 1. Further, the analysis informs the control mechanisms needed to mitigate cybercrimes, as discussed in Table 2.

a) Analyse the CTI gathered in phase 1, regarding how the Ransomware attack was deployed.
b) Assess the impact of a Ransomware attack and its cascading impact on current profiles, servers, reputation, legal and cost.
c) *Sub Phase:* We may use SWOT analysis, Digital forensics results, and the attack models to reduce cyberattacks to organizational goals.
d) *Review Security control mechanisms to improve on existing policies.*

4.4.5 Respond

This phase seeks to develop measures to protect, mitigate and implement countermeasures to safeguard the organizational assets. These include Assess Controls, IT/IS Auditing, Backups, Data Security and Information protection, contingency planning, CERT, Policies, and Procedures in line with international standards.

a) *Sub Phases:* Provide training and workshops for staff.
b) Ensuring best practices, and
c) Certifying systems using recognized standard institutions such as (ISO207002, ISO27005 and NIST 2018).

5. Discussion And Recommendations

Evolving organizations have integrated their organizational requirements, business process and information flows to SMEs and third-party vendors in a supply chain environment for global demands and competitive advantage. That has led to various threats, risks and vulnerabilities in the organizations as cybercrimes exploit these vulnerabilities using Inland hooping and advance persistent threat attacks. Mitigating these cybercrimes has been a significant challenge due to the unpredictable nature of cyberattacks. Thus, integrating the framework phases into an attack model will assist in identifying organizational assets, attacks, and threats to protect the organization. We determine the attack vectors using subjective expert opinions to determine how threats propagate. The CCMF model derives concepts from NIST 2018 Cybersecurity Infrastructure framework. The five phases include:

5.1 Identify, Assess, Analyze, Evaluate and Respond

The identification phase is a strategic management imperative. First, a security team is appointed to identify all the assets, vulnerable spots, and probable threats that exploit the organizational assets. Further, an organization may connect part of its network infrastructure to an external organization and third-party vendors. Thus, an external audit may be required to mitigate the other network nodes connected to the system. For instance, ISO 27002 ISMS and ITIL4 guiding principles consider factors required to identify organizational assets and infrastructures. Finally, the assessment phase includes risk assessment concepts. It is expected that an organization may experience uncertainties that, should they occur, may impact the organization's goal, objectives, business process, and product. For instance, (ISO/IEC 27005, 2011; ISO 31000, 2018) provide the scope, context, framework, and techniques required to mitigate organizational risk. A proactive risk assessment prevents cybercrime occurrences rather than a reactive assessment. However, implementing them provides assurance, improved configuration mechanisms, awareness, training, and control. The analysis phase considered the approaches deployed by an adversary and the attack pattern and vectors used. The rationale is to understand cybercriminals' methods, opportunities, and motives. Furthermore, the analysis and understanding of the attack pattern and vectors provide situational awareness and assist in configuration mechanisms during security implementations. For instance, in the case of a ransomware or malware attack on an organizational system.

We used Table 1 to analyze the method used to deploy the attack by identifying the following attack step, attack analysis, attack vectors, and mitigations: A malware analysis will reveal that an attacker can attach a worm in a phishing or spear phishing email and send it across. Then, when any victim opens the attachments, the worn will activate. Further, in an event where a remote access trojan has been deployed, regularly changing the password as a mitigation factor will reduce the number of accesses that the attack may have to exploit. Further, cyber security research requires that we provide probabilities and assumptions since, there is no single research that has all security control and solutions in the evolving threats and vulnerabilities landscape in the event of an attack. Table 1 considers areas that may be vulnerable to attacks in evolving and integrated networks as follows. For instance, the malware analysis related to a phishing attack will reveal that an attacker can use a phishing email with malware attached to gain access to a network. However, changing passwords regularly can prevent the attacker from remaining in the system permanently. Thus, it is relevant for mitigating cybercrimes.

Table 1. Cybercrime Attack Analysis Steps

Steps	Attack Analysis	Attack Vectors	Mitigation
1	Determine the nature of Ransomware or Malware	Logic Bomb, Virus, Trojan, Phishing, Time bomb, Macros, Virus	Software Updates, Anti-Virus, implement configurations, Change Password Regularly.
2	Actual sources of the Virus	Malware Installed or Malware Executed	Detect sources of Emails and Attachments. Prevent Virus Replications Using IDS/IPS
3	The subject of the Virus used by the attacker	Urgent Request, Payment Suspended, Management Meeting, Payroll, Follow Up, I Love You Bug, Direct Debit	Use a Specific Firewall. E.g. Deep Packet Inspecting or Filtering Firewalls for detections, Packet Analyzer
4	Source of attack Embedded URLs	Organizational website XXS and CSRF attacks, session hijacking, island hopping attack from a third-party website	Implement a policy to monitor contents. For example, configure filters to determine all user inputs on arrival, Block unnecessary websites from accessing URLs.
5	Types of attachments and specific attachments	Phishing or Spear phishing, rootkit, botnet	Implement Multifactor authentication, prevent domain spoofing, Install anti-malware security software
6	Analyze if there are any links affected	Is the Virus linked to other sources	Implement filters to detect all network nodes and points of sale.
7	Determine how malicious the virus impact is	Cascading impact on third parties connected to the organization	Carry out internal and external audit trails to align security goals.
8	Identify if the Virus sent has spread to others	Determine the effects on others	Implement Mitigation factors such as Insurance, accept, or avoid the risk
9	Identify Commonalities of who and what has been targeted	Motive and intent of the cybercrime	Gather threat intelligence to understand the threats and the criminal's mindset for situational awareness and security strength state.
10	Determine if malicious attachments were opened or links followed	Staff that opened the attachment and those connected to each department.	Implement subnetting and internal firewalls to minimize and contain the spread.

11	Analyze and Evaluate the Virus	Nature of Virus, worm, or trojan deployed by the attacker	Carried Impact Analysis and evaluation of security strength on a regular or Adhoc basis.
12	Report Findings	Indicate assets, attacks, vulnerabilities, risks, and threats to the organization. Indicate attack patterns, vectors, and exploits. Provide recommendations, Generate an Audit report.	Approve reports, organize training and workshops, Certify systems, Formulate policies, and Improve security control requirements and configuration mechanisms. Develop information-sharing platforms with stakeholders.

5.2 Security Controls

Table 2 highlights the recommended controls required in line with the framework phases, as discussed in sections 4.4.1 to 4.4.5, to provide operational security and assurance to the organization's assets and infrastructures. Security control mechanisms are integral to effectively mitigating cybercrimes to ensure business continuity processes and information flows. Control objectives has been aligned with the proposed framework phases and standards including directive, preventive, detective, corrective, and recovery controls. The control objectives are implemented to identify vulnerabilities, attacks risk threats and analyze and evaluate strategic management decision-making. In addition, the objectives specify standards, policies, plans, and procedures required to monitor and mitigate the attacks, risks, and threats to the systems. Further, it assigns security ownership to management to maintain continuous improvements to security requirements and ensure policies, procedures, and practices are enforced across the organization. Table 2 provides a matrix of recommended security controls.

Table 2. Recommended Security Controls

Controls	Framework Phases	Summary	Standards
Directive	Respond	Oversees the strategic, tactical, and operational security requirements and respond accordingly. That includes authorizing standards and policies. It is a control intended to provide guidance and training to advise employees of the expected behavior during their interfaces with or use of the organization's information systems.	ISO 27002 ISMS. (2017): Section 5.1.1 Provides Management Directives and support for information security in line with business requirements, laws, and regulations. ISO/IEC 27005: Risk Management Strategy required for the risk objectives ITIL 4: Provide guidelines for strategic decision-making. NIST Cybersecurity Framework, (2018): Standards, Policies, and Guidelines for the components
Preventive	Evaluate	Implement preventive controls required to prevent the limited probability of attacks and undesired outcomes to physical infrastructures, administrative and technical measures intended to preclude actions violating policy or increasing risk to system resources.	ISO 27002 ISMS. (2017): Support for the framework Cores and Implementation Tiers OWASP Proactive Control 2018: Technical Guide for Mobile Web App NIST Cybersecurity Framework, (2018): Provides Technical Implementation and uses five functions to identify controls catalog.
Detective	Analysis	Detective controls involve using practices, processes, and tools (IDS/IPS, Firewalls, Anti-malware) to identify cybercrimes, fraud, errors, authorized access, and penetrations that may react to security violations.	ISO 27002 ISMS. (2017): Support for the framework Cores and Implementation Tiers NIST Cybersecurity Framework (2018): Use five functions to analyze the entire risk management profile ISO/IEC 27005: (2011): Provides Risk Mitigation Techniques ITIL4: Provides IS risk mitigation for service value chains

Corrective	Assess	Corrective controls to correct unexpected outcomes, risks, and zero-day attacks on physical infrastructures. Technical measures and configurations are designed to react to the detection of an incident to reduce or eliminate the opportunity for the unwanted event to recur.	NIST SP 800-161r1 (2022) Provide CSC Risks Assessment NIST Cybersecurity Framework, (2018): Use the implementation Tiers and the subcategories to risk tolerance ISO 27002 (2017) Secure Development Environment ISO/IEC 27005 (2011) Risk Assessment Process for ITIL4: Provides IS risk mitigation for service value chains
Recovery	Identify	Recover systems to the operational level when an incident occurs that compromises integrity or availability. The implementation of recovery controls is necessary to restore the system or operation to a normal operating state.	NIST 800-161r2 (2012): Provide Incident Handling Guide in the event zero-day day attack NIST SP 800-61r2 (2012): Provide Back information to organizations ISO 27002 (2017): Provide Backup Objectives against data loss.

6. Conclusion

Organizations have evolved using the internet to improve their business processes, increase production speed and reduce the cost of distribution by integrating their small and medium-scale enterprises (SMEs) and third-party vendors. Further, using online services has brought benefits such as increased online services, increased global market share, collaborations, online payments, and delivery in a an integrated network environment. However, these integrations has led to increased cybercrimes exponentially with adversaries using various Advanced Persistent Threats (APT) methods to penetrate and exploit the organizational threat landscapes. Thus, mitigating cybercrimes in an evolving organizational landscape has become unavoidable.

The paper has discussed some of the existing challenges leading to evolving threat landscape and the vulnerabilities influencing cybercrime threat. Factors leading to such vulnerabilities include inadequate attack modelling to mitigate attacks, security misconfigurations, and inadequate cyber threat intelligence gathering to create situation awareness, that are exploitable by these criminals are some of the key factors leading to the practical implications in mitigating cybercrimes. We have reviewed related literature that considers cybercrime frameworks and proposed a model for mitigations. The CCMF phases consist of five key components for the mitigation processes required throughout the life of a business. Mitigating cybercrimes in an evolving organization landscape has become could improve integrated network systems with other organizations' internet to improve organizational security requirements and business process collaborations. We have considered the concepts of threat modelling from the implementation section and developed the proposed Cyber Crime Mitigation Model (CCMF). The domain phase includes Identify, Assess, Analyze, Evaluate and Respond. We identified organizational assets, attacks, and threats. Further, we develop a proposed cybercrime framework that provides a common language platform for the approach, guidance, concept, and implementation of cybercrime mitigation in an organizational ecosystem. The framework domain provided phases to prevent cybercriminals from penetrating, infiltrating, manipulating, exfiltrating, and obfuscating using APT and Command control methods.

Finally, we model the framework phase that provides the principal set of basic requirements to guide to achievement of the risk-mitigation outcomes. It includes the framework domain, phases, sub-phases, and standard references. We continue further to improve the framework development. Subsequently, we proposed a matrix that can be used to analyze the methods used to deploy attacks by identifying the attack steps, attack analysis, attack vectors, and mitigations from existing standards.

6.1 Comparing our Work with Related Works

Comparing our work with other related works, NIST (2018) proposed a theoretical framework for cybersecurity using four implementation tiers ranging from Partial Tier 1 to Adaptive - Tier 4. (NIST 2018). OWASP ASVS, (2021) proposed a method for establishing and using repeatable security processes and standard security controls. (Razzaq et al., 2014) proposed a methodology to approach web application security. The Information Security Management Standards (ISMS) framework (ISO27002: 2017) provides security standards, guidelines, and implementing controls. However, the framework may only meet some organizational security requirements as it is broad and specific to satisfy security objectives. MITRE proposed a kill-chain attack model and framework that describes the steps used by the adversary to compromise and operate within an organization's network (MITRE, 2013), among others. All the models and frameworks in the related works are relevant and generic to cyberattacks and contribute to cyber security. However, the works did not consider specific cybercrime mitigating frameworks relevant to an organizational threat landscape to improve security.

Future works will consider applying machine learning techniques on classification models to learn a dataset to learn for performance accuracy and cybercrime threat predictions using case studies to predict future trends in evolving organizations. Further, work will consider applying the CCMF model to analyze and detect cyberattacks and risks in a cyber supply chain systems resilience.

References

Ahmed, A. S. Deb, S. Bin Habib,A. Z. S., Mollah, Md. N. and Ahmad, A. S. (2018) "Simplistic Approach to Detect Cybercrimes and Deter Cyber Criminals," in the 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2), Rajshahi, Feb. 2018, pp. 1–4. doi: 10.1109/IC4ME2.2018.8465618.

Anderson, R.J., Barton, C.J., Böhme, R., Clayton, R., Eeten, M.V., Levi, M., Moore, T.W., & Savage, S. (2012). Measuring the Cost of Cybercrime. *Workshop on the Economics of Information Security*.

Anderson, R., Barton, C., Boehme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., et al. (2019). Measuring the Changing Cost of Cybercrime. *The 18th Annual Workshop on the Economics of Information Security* https://doi.org/10.17863/CAM.41598.

Back, A and LaPrade, J. (2019) "The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence," Int. J. Cybersecurity Intell. Cybercrime, Sep. 2019. vol. 2, no. 2, pp. 1–4.

Bank of Ghana (2016), "CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations" https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf.

Bischoff, P. (2020)"Ransomware attacks on US healthcare organizations cost $20.8bn in 2020," Comparitech, Feb. 11, 2020. https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/ (accessed Aug. 27, 2021).

Bissell, K., Lasalle, R., and Cin, P. D. (2022) "State of Cybersecurity Report 2020 I Accenture"[Online]. Available: https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf (Accessed: Aug. 17, 2021)

Brewster, T. (2021) "Ransomware Hackers Claim To Leak 250GB Of Washington, D.C., Police Data After Cops Don't Pay $4 Million

Ransom," Forbes, 2021. https://www.forbes.com/sites/thomasbrewster/2021/05/13/ransomware-hackers-claim-to-leak-250gb-of-washington-dc-police-data-after-cops-dont-pay-4-million-ransom/ (accessed Sep. 15, 2021).

Camillo, M., Frey, k. & Summers, G. (2012). "Mitigating The Risk of Cyber Crime – Advice For Companies." [Online] https://www.financierworldwide.com/mitigating-the-risk-of-cyber-crime-advice-for-companies#.Y7tnu3bP02w. (Accessed 22 December 2022)

Chaphekar, S. (2019) "COBIT, ITIL and ISO 20000- The Main Differences" (Accessed 12th December 2022) https://advisera.com/20000academy/blog/2019/09/25/cobit-vs-itil-vs-iso-20000-a-comparison/

Dashora, K. (2011)."Cyber Crime in the Society: Problems and Preventions," Journal of Alternative Perspective in the Social Science. Vol 3, No 1, pp. 240–259,

Dwivedi, Y.K., Ismagilova, E.D., Hughes, L.D., Carlson, J., Filierie, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A.S., Kumar, V., Rahman, M.M., Raman, R., Rauschnabel, P.A., Rowley, J., Salo, J., Tran, G.A. and Wang, Y. (2021), "Setting the future of digital and social media marketing research: perspectives and research propositions", International Journal of Information Management, Vol. 59, doi: 10.1016/j.ijinfomgt.2020.102168.

Thorpe, E. K. (2019) "50% of Cyber Attacks Now Use Inland Hopping" July 2019. https://www.itpro.co.uk/security/33946/50-of-cyber-attacks-now-use-island-hopping.

FinanceOnline, "16 Latest Cybercrime Trends & Predictions for 2021/2022 and Beyond," Financesonline.com, Oct. 21, 2019. https://financesonline.com/cybercrime-trends/ (accessed Sep. 23, 2021).

Fonseca-Herrera, O.A., Rojas, A.E. and Florez, H. (2021), "A model of an information security management system based on NTC-ISO/IEC 27001 standard", IAENG International Journal of Computer Science, Vol. 48 No. 2, pp. 213-222.

Gercke, M. 2012. Understanding Cybercrime: Phenomena, Challenges and Legal Responses. ITU Telecommunication Development Bureau. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Accessed 6th September 2012.

Hannibal, C., Rowan, J., Durowoju, O., Bryde, D., Holloway, J., Adeyemi, O. and Shamim, S. (2022), "Who shares wins? Understanding barriers to information sharing in managing supply chain risk", Continuity & Resilience Review, Vol. 4 No. 2, pp. 161-175. https://doi.org/10.1108/CRR-11-2021-0038.

Hitchcox, Z. (2020), "Limitations of cybersecurity frameworks that cybersecurity specialists must understand to reduce cybersecurity breaches", Colorado Technical University ProQuest Dissertations Publishing, ProQuest LLC, Ann Arbor, Michigan. https://www.proquest.com/openview/94ad5f8c6d410e440a39b865b5f042aa/1?pq-origsite=gscholar&cbl=44156#:~:text=The%204%20major%20themes%20identified,d)%20compliance%20is%20not%20security. (Accessed 27th February 2023)

ISO/IEC 27002 (2017), "Information technology Security techniques Code of practice for information security controls." https://www.iso.org/standard/75652.html

ISO/IEC 27005 (2011) "Information technology Security Techniques Information Security Risk Management." SAI Global.

ISO/IEC 27005 (2011) "Information Technology Security Risk Management. International Organization for Standardization" Geneva, Switzerland. https://www.iso.org/standard/75281.html

ISO, (2018) Risk Management Guidelines. https://www.iso.org/standard/65694.html.

Kaspersky (2021), "Tips on how to protect yourself against cybercrime," Tips on how to protect yourself against cybercrime, 2021. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Leal, R (2016) “ISO 27001 and ITIL: Similarities and Differences” Adviser. (Accessed 14th December 2022) https://advisera.com/27001academy/blog/2016/03/07/iso-27001-vs-itil-similarities-and-differences/

Leyden, J. (2017) “UK vuln 'fessing pilot's great but who's going to give a FoI?” https://www.theregister.com/2017/03/22/uk_gov_vuln_disclosure_pilot/. (Assessed 14th June 2022)

Mokha, A. K. (2017), "A Study on Awareness of Cyber Crime and Security," Res. J. Humanit. Soc. Sci., vol. 8, no. 4, p. 459, 2017, doi: 10.5958/2321-5828.2017.00067.5.

Morgan, S. (2019), “Official Annual Cybercrime Report: Cybercriminal activity is one of the biggest challenges humanity will face in the next two decades," HERJAVEC GROUO, 2019. Accessed: Aug. 17, 2021. [Online]. Available: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Morgan, L. (2021) "IOTW: University of California Schools Hit with Ransomware Attack," Cyber Security Hub, Apr. 30, 2021. https://www.cshub.com/attacks/articles/iotw-university-of-california-schools-hit-with-ransomware-attack (accessed Sep. 15, 2021).

Morgan, S. (2020) "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime Magazine, 2020. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (accessed Aug. 17, 2021).

MITRE (2013) "Threat-based Defense," Jul. 2013 [Online]. Available: https://www.mitre.org/capabilities/cybersecurity/threat-based-defense, (Accessed: Sep. 24, 2021)

Nabe. C (2021) Impact of COVID-19 on Cyber Security. Deloitte. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html. (Accessed 3 December 2022).

Nadir, I and Bakhshi, T (2018) "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques," in 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Mar. 2018, pp. 1–7. doi: 10.1109/ICOMET.2018.8346329.

Nguyen, T. V. (2020) "Cybercrime in Vietnam: An Analysis based on Routine Activity Theory," Int. J. Cyber Criminol., vol. 14, no. 1, pp.156–173.

NIST Cybersecurity Framework (2018) “Framework for Improving Critical Infrastructure Cybersecurity” Ver1.1. https://doi.org/10.6028/NIST.CSWP.04162018 (Accessed May 2021)

NIST SP 800-61r2 (2012) "Computer Security Incident Handling”12, 2013. http://dx.doi.org/10.6028/NIST.SP.800-61r2 (Accessed Sep. 15, 2022)

NIST (2018) "Framework for Improving Critical Infrastructure Cybersecurity," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Accessed Sep. 15, 2022

NIST SP 800-161r1 (2022) “Cybersecurity Supply Chain Risk Management Practices for Systems and Organization.” https://doi.org/10.6028/NIST.SP.800-161r1

NDC News, (2021) "Impact of Ransomware Attack on Mass. Steamship Authority Expected to Continue Thursday," NBC Boston, 2021. https://www.nbcboston.com/news/local/mass-steamship-authority-delayed-due-to-cyber-attack/2395477/ (accessed Sep. 15, 2021).

Ozdemir, Y., Basligil, H., Alcan, P. and Kandemirli, P. (2014) “Evaluation and Comparison of COBIT, ITIL and ISO27k1/2 Standards Within the Framework of Information Security,” International Journal of Technical Research and Applications, vol. 11, pp. 22–24.

OWASP (2021), "OWASP Top Ten Web Application Security Risks | OWASP," https://owasp.org/www-project-top-ten/. Accessed September. 15, 2021).

OWASP ASVS (2021), “Application Security Verification Standard” https://owasp.org/www-project-application-security-verification-standard/ (Accessed 20th December 2022)

OWASP Proactive Controls, (2018) https://owasp.org/www-project-proactive-controls/. (Accessed 20th December 2022)

Pawar, S. and Palivela, H. (2022), “LCCI: a framework for most minor cybersecurity controls to be implemented for small and medium enterprises (SMEs)”, International Journal of Information Management Data Insights, Vol. 2 No. 1, doi: 10.1016/j.jjimei.2022.100080.

Razzaq, A., Anwar, Z., Ahmad, H. F., Latif, K., and Munir, F. (2014) "Ontology for attack detection: An intelligent approach to web application security," Computer Security., vol. 45, pp. 124–146, Sep. 2014, doi: 10.1016/j.cose.2014.05.005.

Sucuri, A. (2021) “OWASP Top 10 Security Vulnerabilities 2021,” Sucuri, 2021. https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2021/ (accessed Sep. 15, 2021).

Sattar, Z., Riaz, S., Shafia, and Mian, A. U. (2018,) "Challenges of Cybercrimes to Implementation of Legal Framework," in 2018 14th International Conference on Emerging Technologies (ICET), Islamabad, Nov. 2018, pp. 1–5. doi: 10.1109/ICET.2018.8603645.

Summerville, A (2017), "Protect against the fastest-growing crime: cyberattacks," CNBC, Jul. 25, 2017. https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html (accessed Sep. 15, 2021).

TechTarget Contributor (2020), “Island Hopping Attack” https://www.techtarget.com/whatis/definition/island-hopping-attack (Assessed, 2nd January 2023)

The Auditor General of the Department of Health (2017) “Investigation: WannaCry cyber attack and the NHS” [Online] https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf. (Accessed 15th December 2022)

Touro, T. C. College, (2020), "The 10 Biggest Ransomware Attacks of 2021," Touro College Illinois, Jun. 10, 2020. http://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php (accessed Aug. 27, 2021).

Thomas, G. and Sule, M.-J. (2022), "A service lens on cybersecurity continuity and management for organizations’ subsistence and Growth,” Organizational Cybersecurity Journal: Practice, Process and People, Vol. https://doi.org/10.1108/OCJ-09-2021-0025

The Economist, (2018) “British Airways Faces a £183m Fine Over a Data Breach. [Online] https://www.economist.com/gulliver/2019/07/08/british-airways-faces-a-ps183m-fine-over-a-data-breach?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18156330227&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=CjwKCAiAwomeBhBWEiwAM43YIHhy-SI7yLviVacTHQppKIj4mMvMPQhnHenz8H1CTNGrxAtyZxyaKRoCBh0QAvD_BwE&gclsrc=aw.ds

Paul, K. (2021) “Twitch Hack: Data Breach Exposing Sensitive Information” [Online] https://www.theguardian.com/technology/2021/oct/06/twitch-hack-data-breach-gaming-platform (Assessed 20th October 2022)

Reuters (2021) "Meatpacker JBS says it paid the equivalent of $11 mln in a ransomware attack," Reuters, Jun. 10, 2021. Accessed: Sep. 15, 2021. Available: https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/

Verizon, (2021) DBIR: Data Breach Investigative Report," 2021. Accessed: Aug. 17, 2021. [Online]. Available: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Yeboah-Ofori, A. Y. and Brimicombe, A. (2019) "Cyber Intelligence & OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media A Systematic Review," Soc. Digit. Inf. Wirel. Commun., 2017, Accessed: Aug. 30, 2021.

Yeboah-Ofori, A., Abdulai, J. D. and Katsriku, F (2019) "Cybercrime and Risks for Cyber Physical Systems," Intemational. Journal of Cyber-Security and Digital Forensics, vol. 8, no. 1, pp. 43–57, 2019, doi: 10.17781/P002556.

Yeboah-Ofori, A., Swart, C., Opoku-Boateng, F.A. and Islam, S. (2022), "Cyber Resilience In Supply Chain System Security Using Machine Learning For Threat Predictions,” Continuity & Resilience Review, Vol. 4 No. 1, pp. 1-36. https://doi.org/10.1108/CRR-10-2021-0034

Zappa, F. (2014). “Cybercrime: Risk for the Economy and Enterprises at the EC and Italian Level.” United Nations Interregional Crime And Justice Research Institute (UNICRI)

Zetter, K. Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid. Available online: https: //www.wired.com/2016/03/inside-cunning-unprecedented-hackukraines-power-grid/ (accessed on 18 December 2022).