Security Professionals Must Reinforce Detect Attacks to Avoid Unauthorized Data Exposure

Alain Loukaka[1] and Shawon S. M. Rahman[2]

Abstract - Organizations face the probability of being hacked because of weak and inadequate cybersecurity implementations. Hackers are still able to breach a system when security tools such as firewalls, SIEM, anti-virus software, encryption, and IDPS are readily in place within an organization. Digital criminals are responsible for increased network breaches using elusive security tools to penetrate secure environments with sophistication. Cyberattacks are continually increasing due to the sophistication and innovation of cyber attackers. Many vulnerable areas must be reinforced against cybercriminals, Insider threats, inadequate employee training, and negligence. Monetary investment in cybersecurity and management support plays a significant role in assuring the implementation of information security throughout any organizational processes. The implication for practice can provide organizations with approaches on how to mitigate cyber exploits and safeguard the confidentiality, integrity, and availability of information by bridging the gap between incident detection and response.

Keywords - Data Breach, Computer crime, Cyberattack, Exploit, Hacking, Zero-day attack

1. INTRODUCTION

Information security has become so essential that organizations must implement safeguards to protect their internal assets and intellectual property [1]. Organizations need to plan comprehensively against cyber theft [2]. Understanding the nature of security threats will help organizations effectively apply the proper security measures to protect their assets and harden their network [3]. Precautionary steps must be taken to formulate viable solutions against cyber-attacks [4]. New opportunities to steal information digitally continuously emerge. Because of the increasing rate of breaches, information security importance has increased [5]. Digital criminals impact organizations' revenue due to the loss of customers and business partners [6].

[1]Capella University, Minneapolis, MN, USA
[2]Department of Computer Science and Engineering University of Hawaii-Hilo, Hilo, Hawaii, USA

Security vulnerabilities are continually exposed, and attacks are repeatedly formulated to bypass recently applied countermeasures [4]. Current cybersecurity countermeasures are not enough to mitigate the risks associated with digital crimes [7].

Hackers use intricate techniques to infiltrate network systems to acquire and steal sensitive information [8]. Social engineering, network exploits, malicious coding, and human factors are exploitative methods making the fight against cyber theft imperative [9]. Many organizations have internal security in place, but technical controls do not entirely prevent thefts as demonstrated by high-profile breaches such as Sony and Equifax. Organizational management often does not have security in mind – it is only an afterthought, and unfortunately, many incidents are detected months after the initial breach occurred [1][10]. Organizations must put more emphasis on security because cyber threats and security incidents affect the economy and cost billions of dollars in remediation [2]. Employee responsibility is a critical element to strengthen an organization's cybersecurity. About half of all security breaches have been initiated or facilitated internally, whether intentionally or unknowingly [11]. Moreover, zero-day attacks are active because countermeasures are unavailable to the organization [12]. These attacks are challenging to detect due to their unknown nature and characteristics. Cyber breaches are now proliferating at a fast rate, and hardening organizational networks are imperative [3]. The impact cybercriminals have on the economy is detrimental and growing year after year [13].

The literature indicates known security-related study gaps related to the lack of communication and cooperation about cyber threats between organizations exist [14]. Also, there are security gaps between cybersecurity measures and countermeasures and how to efficiently mitigate cyber risk exposure [15]. The literature also indicates the difficulty mitigating cyberattacks such as zero-day attacks because of hackers' sophisticated penetration techniques [16]. Security tools such as firewalls, SIEM, IDPS, and antivirus software are not equipped to detect and eradicate harmful exploits. Insider threats are another

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

area worth exploring since they cause more than 50% of all reported breaches [11]. Corporate training, stronger security policies, and control measures such as vacations, least privilege, and separation of duty are significant security contingencies [17]. The research literature also indicates that cyber threats are increasing, impacting organizations financially, sophisticated, but there is no definitive application to mitigate exploits with efficacy to prevent further infrastructure breaches.

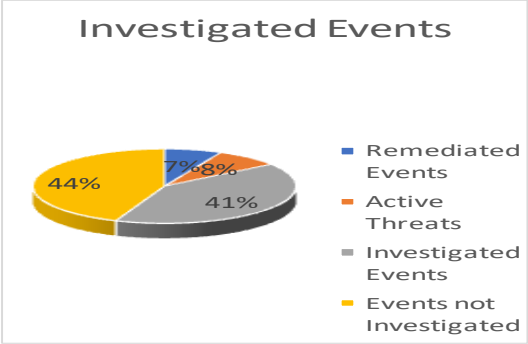

Figure 1 Event Analysis

2. Literature Review

2.1. Exploits Effect

Cybersecurity is a global concern because it increases the need for more information systems and services [18]. The need for cybersecurity measure improvement comes from the relentless new attack techniques employed by hackers to gain access to customer information [19]. Cybercriminals, such as a hacker or cyber thief, are individuals using technological tools and hardware to launch coordinated attacks to exploit a system(s) based on their vulnerabilities. Those individuals respectively use codes to affect the targeted machines to infiltrate and extract the data for the future and using hardware such as a tablet, computer, or phones to perform their attacks. Organizations must apply the necessary deterrent from patching, software, and OS updates, scanning, and monitoring to make sure the infrastructure is protected and less vulnerable and attractive to cyber thieves. Cybersecurity professionals must have a deeper understanding and knowledge regarding security attacks, their detection, countermeasures, and remediation [20]. Cyber incidents are dominant in recent years and affect organizations in government, healthcare, education, and businesses. Specific strategies must be incorporated because of cyber threats' continuous increase [21]. Sophisticated cyber exploits illegally penetrate organizations around the world [22]. The more valuable the data is, the more certain malicious users want to extract the information. Stealing data is the essence of digital thieves [23]. Because cybersecurity has become an important topic, the information technology (IT) research advisory company, Gartner Inc., estimated security-oriented spending would dramatically increase, reaching $96 billion in 2018 [24]. The negative impact of cyber threats necessitates making infrastructure as secure as possible. Security awareness throughout the organization is imperative. Keeping abreast of current exploitation techniques, such as social engineering, is essential. Many individuals do not understand the tactics used by hackers to get into systems, such as spam, viruses, or the use of authority. Network attacks are on the rise with no sign of cessation.

2.2. Exploit Economic Impact

The emergence of complex types of cyberattacks such as extortion using ransomware is aimed at exploiting vulnerabilities in the Internet of Things and voting systems. With the use of the anonymous nature of bitcoins, cybercriminals have become dangerous and hard to trace the crypto-currency activities [25]. Many of the ransomware attacks are still arriving through emails, and many employees are still not adequately trained to recognize malicious emails. Ransomware attacks are prevalent in education, IT, entertainment, and financial areas with an average of 22% [25]. Cybersecurity is becoming a growing challenge for organizations, and solutions must be formulated to keep pace with growing cyber threats [26]. Security breaches affect many organizations, resulting in financial losses [27].

Cybercrimes are financially motivated attacks and are always successful and increasing more frequently for the past decade [28]. Online threats are continuously evolving for 6762 breaches that occurred in 2016 alone [28]. Fifty percent of breaches originate internally [29]. Cybercrime costs United States businesses more than $250 billion and as high as $1 trillion worldwide [30]. Reducing the number of security violations is a significant step toward secure systems. The impact of cyber threats resonates within organizations worldwide, and stolen data cost billions of dollars post-security incidents. There is a lack of documentation on digital protection and enhancement regarding the detection process [31]. Between 2011 and 2013, breaches increased from 42% to 81%. Digital attackers steal information for financial motivation, which yields millions of dollars in theft [32]. Cybercrime yields more than $1 trillion worldwide, with each attack generating between $50 billion and $120 billion economic impacts on the targeted organization [33]. Online threats are continuously evolving for 6762 breaches that occurred in 2016 alone [28]. Fear of a cyberattack and data exploit is a constant reality for businesses and government agencies [34].

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

2.3. Human Impact

Organizations must understand the impact of human behavior that contributes to insider threats, whether intentionally or not [35]. Human errors cause harmful activities by allowing cyber thieves to exploit the vulnerability of the system due to either security system misconfiguration or mismanagement [36]. Individual behaviors are the cause of rising internal threats because security procedures are violated [37]. Insider threats account for more than half of all intrusions in a system. Knowing the state of the infrastructure and the integrity of employees is imperative. The potential security threat posed by disgruntled employees with unethical behavior must be addressed with proper security measures. Internal cybersecurity employees do not identify an ongoing breach accurately because implemented security measures are neither adequate nor current [37]. The distinction between insider and outsider threats is a challenge but also an opportunity to explore better security controls to eliminate cyber threats more consistently [38]. Organizations must pay closer attention to outsider threats because 50% of breaches are caused by them [39]. Sociological and psychological understanding of employee behaviors is an area for further study. Understanding and controlling human conduct are essential to identify future internal security problems. Because more attacks originate internally, better strategies must be in place regarding the misconfiguration of internal security systems [17]. Immediate improvement of detection methods must be implemented. IDPS configuration plays a significant role in cyber exploit countermeasures [36]. The answer is to formulate a practical security technical solution for implementation. The distinction between authorized and unauthorized users is difficult to assess [17]. The ability of malicious users to avoid capture has become more sophisticated. Hackers can effectively avoid detection while exploiting the system and modify logs. System hardening can manage the prevention of further security incidents. The mitigation of external and internal attacks is imperative with elaborated countermeasures.

Goal-persuading behaviors within an organization must be used to promote efforts to safeguard security systems [40]. Protection motivation theory (PMT) is a cognitive process that explains fear appraisal and its mediating behavioral change [41]. Two major cognitive mediating processes exist in PMT: the threat appraisal and the coping appraisal processes. Respectively, they are the appraisal of an individual to recognize the threat and its possible coping behaviors, threat severity, vulnerability, and rewards. PMT can help an individual understand the repercussions of their actions based on their efforts to promote ethical practices. Organizations should develop an understanding of a hacker's motivations and probably involve professional hacker expertise [8]. The role of managers is essential to address the issues organizations are continually facing [2]. The National Security Agency (NSA) is deeply affected by the vast internal amount of secret information leaks [42]. Many hacking cyberweapons were exposed to social media, Twitter, by a group of hackers named Shadow Brokers. Highly sensitive information was disclosed with classified operations that were conducted. The Snowden case, a CIA employee, who disclosed information to journalists about how the government used unique codes later decipher by the Shadow Brokers group. Then, those cyberweapons were in the hands of North Korea and Russian and used to attack the United States. The cyberspace is now full of emerging and innovating techniques that facilitated the rise of social media, cloud computing, smartphone technologies. Cyber attackers must be stopped, and organizations must regard security has the most critical aspect of their infrastructure to avoid costly catastrophic events such as ransomware. Implementing the right tools to aid in the detection, protection, and remediation within the network security system is crucial. Cyber exploit is a worldwide phenomenon that continues to threaten organizations. Many hacking groups, such as the APT40, are emerging to stealing secret and intellectual property from various states like China [43]. The level of espionage from the APT40 group is highly sophisticated and successful. The group's ability to access privileged information is formidable since zero-day vulnerabilities were not in use yet to perform attacks.

2.4. Digital Crime Management

Hackers are successful because they meticulously scope the infrastructure to infiltrate the system. Poor information security led to the compromised data of over 600 Galaxy Samsung users at Home Depot, Goodwill, Target, and many more. It is imperative to improve cybersecurity performance to combat the increasing sophistication and stealth approaches of malicious individuals compromising a system. The following study concurs with the Verizon data breach report that shows insiders caused 62% of breaches [44] The report also demonstrated that 60% and 53% of threats were from Asia and Australia, respectively. The Identity Theft Resource Centre (2017) identified 850 breaches that resulted in 16 million exposed records [45]. There was a noticeable decline in the impact of offenses compared to 36 million in 2016. The investigations on how to minimize the effects of false-positive and true negative alerts are critical. The development of tools and techniques beyond currently used methods is desirable. Capitalizing on better opportunities to manufacture better technologies to combat cyber threats is essential. Investing in security is imperative. The use of a probabilistic classifier to utilize expert knowledge and assign values to a Bayesian

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

network model was employed. The conducted experiment led to the improvement of alert management for intrusion detection and helped detect irregularities in IDPS. This discovery is critical to confront DoS attacks. Identifying DoS attacks is more crucial and complicated since botnets infect computers to activate a DDoS from multiple locations [46]. The study revolves around the adoption of a divided two-part adaptive system (DTPAIDS) to reduce the high level of false-positive alerts. DTPAIDS can track changes within information behavior, data reformatting, and alerts counters. Employing this method enhances the performance and integrity of the warnings triggered. The study shows a reduced error rate of about 4.02%. The false alert rate is significantly reduced among authorized users. Since the analyzed data must be in real-time, alerts must be triggered at once to diminish potential intrusions. Because of the vast number of warnings and the significant resources needed, an investigation into all the activities is not completed [47]. Data post-intrusion is usually not recoverable or usable. The implemented conventional methods such as firewalls, IDPS, SIEM, encryption, and antivirus software are just not enough. Using penetration testers to demonstrate how vulnerable the network is can be beneficial to detect malicious unknown coding. Because ethical penetration professionals use the same techniques as malicious individuals, gathering critical intelligence information on how to counter those attacks is essential [48]. Management must decide what type of test would be allowed (pen, white box, grey box, or black-box tests, and vulnerability assessment) [49]. Organizations must protect their critical information infrastructure by employing accurate cybersecurity measures and threat intelligence [50]. Hackers will use any technical means to penetrate and render a powerless system crippled unless their demands are met in the form of payment (Ransomware) in most cases. As shown in Figure 2, the risk assessment depicts the constant battle to an organization regularly faces [51].

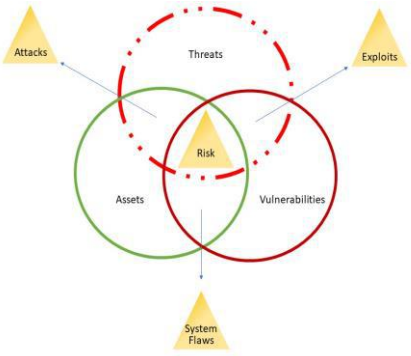

Figure 2. Risk Assessment.

The figure shows the correlation between threats, vulnerabilities, and assets and how risk is the primary element to links them all. The risk encapsulates the potential impact of attacks, exploits, and system flaws to be addressed to secure the system. Stringent security detections are imperative to alert unauthorized access immediately. Thieves are now able to perform attacks from anywhere in the world. Cyber theft's evolving resume requires organizations to concentrate more on security than just business as usual. Information security must take a more significant role in every aspect of daily business' decisions. The critical asset to any management is data and protecting its integrity, confidentiality, and availability is paramount. Now, in addition to regular business routines, unknown threats and vulnerabilities are daily challenges that organizations must fit in their culture to avoid catastrophic events. However, the adverse growth of the Internet provides a platform for digital thieves to exploit a system internally or externally from anywhere. As depicted in Figure 2, risks, in the middle of the interconnected circles, show how threats and vulnerabilities routinely impact an organization, and how risks, attacks, system flaws, and exploits are used continuously to take advantage of security flaws. Stricter control must be in place to monitor organizational infrastructure. Disgruntled employees' access must be revoked during the off-boarding process. However, the real culprit is the misconfiguration of the system security protocol and measures. The detection of unknown exploits, vulnerabilities, and elaborated attacks is a constant problem. Internal exploits should not be as high, and stricter implemented procedures are indispensable. Hence, analyzing the internal network by detecting and defining vulnerabilities must be the first step. Developing robust security awareness is beneficial. A previous study states that management support is vital to building an elaborate course of action [2].

The ability of hackers to exploit vulnerabilities using social engineering to entice users to perform an unethical action is all too frequent [51]. The idea is to trick users into, mainly, clicking on a link to purposely give away access to their system unbeknownst to the user. Previous studies have focused on the effectiveness of phishing and spear-phishing emails [52][53]. Deception is a significant technology tool a malicious user can use against an unaware person. Steps can be taken at an organization or user level to counter the effectiveness of such attacks. One solution is educating users to avoid opening or clicking on mailing from an unknown sender or source. The organization should use filtering and behavior analysis along with the use of a SIEM, such as IBM QRadar or Splunk, to track anomalous behavior [54][55].

2.5. Future Cybersecurity Recommendations

Security must be taken seriously to tackle cyber threats to enhance security postures and avoid a more

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

magnificent catastrophe in the future [47]. Adapting to new and unknown attacks is critical to prevent hackers from exploiting security measures, especially within behavior and signature analysis. The use of dynamic protocol analysis discovers security breaches more efficient [47]. Organizations employ good security and privacy methods but have never identified future risks associated with security and privacy. For instance, risk management, ethical behaviors, skills, and education have never been at the forefront of any business goals. As a result, the lack of emphasis on those critical areas leaves many unexplored solutions to benefit management positively [27]. Cybersecurity should be the most significant future investment because any organization can be targeted. The best practice is always to remain vigilant and proactive [1]. The initial effort must focus internally on eliminating system deficiencies, whether from an inexperienced professional, disgruntled employee, or unknown vulnerabilities. The best scenario is for organizations to focus on security implementations and employee management [17]. The analysis of the human factors when focusing on internal and external attack origin, along with the ability to efficiently use anomaly detection, is vital [56]. Further understanding of human behavior research can benefit cybersecurity to provide more insights regarding the evolving challenges regarding cyber threats [20]. Regardless of the type of attacks, such as social engineering from hackers, incidents are caused and triggered by individuals. Research in cybercriminal methodology, philosophy, and psychology can contribute to cybersecurity to understand methods used to beat security systems already in place.

Further investments and innovations in technology, normal and malicious user behaviors, ethical culture, education, and training can help prevent threats [57]. The government could propose legislation to push companies to come forward with intelligence to promote better security tools and to share past intrusion incidents or attempts. Sharing information with other organizations is again recommended to address the phenomenon cyber threats have become. The emphasis on information sharing between organizations is an area where security experts recommend further collaboration to address cyber and help companies get ahead and avoid cyber theft and their data exposed. Thus, many other infrastructures can be spared from the same outcome and devastating effects if information about possible or successful risks is publicly shared [4]. An organization can be contaminated with a zero-day attack virus, and their mitigation can be applied to other organizations to detect any security vulnerabilities that might have to allow the cyber exploit to occur. User education and information technology must address the safekeeping of computers and their peripherals. Infected computers are the result of reduced system utilization from users. Understanding the impact of certain viruses and malware is critical to prevent digital infection. DDoS has become a more common strategic attack and has disrupted systems worldwide [46]. The emergence of ransomware attacks has become more frequent and highly successful [58]. Management must align the right policies regarding ethical behavior, operation, and security management [31]. As shown in Figure 3, the Cisco 2017 reports highlight that many events are not thoroughly investigated due to resource challenges and security team constraints [59].

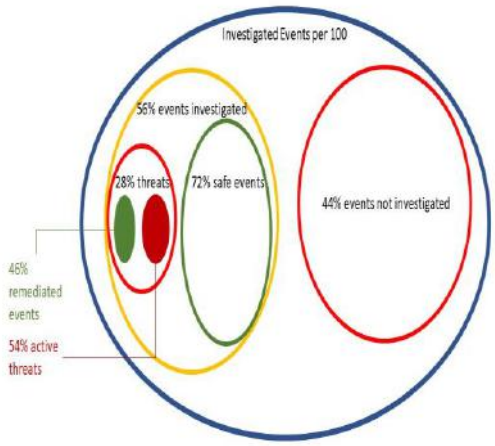

Figure 3. Event Analysis.

Early incident detection can prevent future weeks of remediation, which can be detrimental to a business and its daily operations. Daily traffic analysis shows that 44% of incidents are neither classified nor studied. Among 56% of investigated events, 28% of those classified events register as legitimate threats, but only comprise 46% remediated events, or about 8.5% [59]. Compromised systems are attributed to 59.4% of attacks: 21.4% were via phishing, 12.4% were from ransomware, and 11% were from unauthorized access [60]. Additionally, patching, closing unused ports, firewalls, updating the antivirus, and constant system monitoring is not enough. Figure 4 represents the corresponding increases for the primary designated industries where fraudulent users targeted financial, business, education, and healthcare organizations from 2015 to 2017 [60].

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

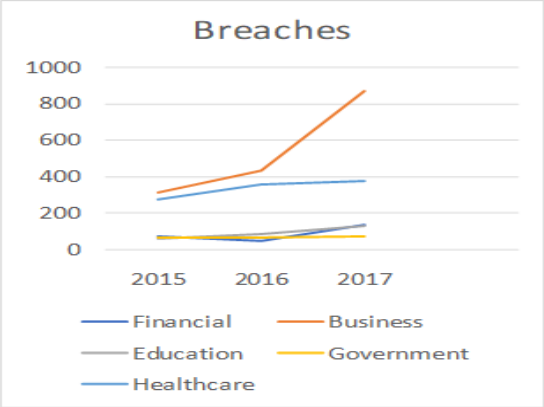

Figure 4. Breaches Analysis.

Users must understand the functionality of the dark side of the Internet, educating themselves and learning how to avoid victimization from various computer crimes such as fraud, espionage, and scams [61]. Social engineering is the most successful type of attack malicious individuals use to compromise a system. For this reason, this exploratory research investigates additional tools to devise an effective cybersecurity countermeasure to stop those attacks, as quickly and as practicably as possible. The study can be beneficial to organizations and add to the core body of knowledge for information security assurance.

3. Security Considerations

The interviews revealed that organizations must establish their degree of risk tolerance and appetite. The investment in the right security component is vital to adequately address the need in areas based on budget and resources. The risk level is essential to be calculated to confront further losses in the future. It is indispensable to understand the value of assets to manage risks efficiently. Management must identify how much to spend on security. Based on the industry sector, organizations should disburse investment accordingly. Management must define the specific risk objectives, what assets to protect, identify asset location, and how to adequately secure them, and the implementation of security updates. There should be a focus on internal and external malicious individuals. Individuals expressed the prohibition of hardware and software access and the use of more cloud-based systems. The previous idea resolution incorporated the use of the least-privilege principle and access controls. The focus also shifted to better physical security and better access control. The method of encryption for offline storage, VPN, robust policy, automation, and avoiding port forwarding are crucial pieces to promote a secure environment. Administrative tools are an additional security layer to help control and manage individuals and identify malicious activities. Management can use separation of duties to disallow the same person cannot have the ability to manage and multiple tasks. A mandatory vacation is helpful to verify an individual followed the proper organization policies. The notion of least privilege is to prevent authenticated users only to have access to minimal resources.

3.1 SIEM (Security Information and Event Management)

SIEMs emphasize the collection and analysis of various event data to provide real-time historical information to facilitate information security [55]. The primary purpose of a SIEM is to collect, report, and correlate events. The critical factors for SIEM success are its analysis ability and to provide insights regarding potential or active security incidents from various sources. ArcSight, RSA enVision, and NetForensics are examples of SIEMs used in many organizations. ArcSight, a Hewlett Packard Enterprise (HPE) SIEM solution, is designed for event threat detection and compliance management. This flexible tool also incorporates currently established security protocols within an organization. RSA enVision is a platform introduced to standardize reports and alerts. The tool provides internal and external audits for security analysis. The instrument achieves two goals: 1) respectively detecting breaches and alerting activities deviating from its baseline, and 2) performs forensic analysis on security events. NetForensics, a SIM (Security Information Management), gathers information from various security devices by providing a rule-based correlation technique to correlate information security among multiple device types. The tool also has customized alerts and reporting for managing an organization's information flow. Splunk and IBM QRadar are among the most-recommended leading network log analysis SIEMs [54]. Splunk helps organizations define and measure their security needs to respond to cybercriminals' persistent attacks.

The software enhances the ability to identify and track traffic within its network by collecting, indexing, and visualizing their log data. This tool also helps to identify criminals and what information they tried to steal from the system. Splunk provides real-time data and is scalable to meet current needs. QRadar is widely used to extend the benefits of 2nd-generation SIEM technology, which is designed to expand visibility within network systems, users, and other applications to provide enough intelligence against potential security exploits. This tool is implemented by significant enterprises to gather and correlate event flow from various locations. QRadar is a scalable product, permitting the integration of other management security tools to enhance detection and analysis. QRadar SIEM and the Network Behavior

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Anomaly Detection (NBAD) engines send their collected events and alerts to the QRadar Intelligence engine, which includes vulnerability scanners, reputation scanners, and threats feed, to the offense SIEM engine [55].

3.2 Encryption

Cryptography is an analytical technique widely used in the digital era and communication sessions. There are a few encryption techniques used to encrypt messages such as the Rivest-Shamir-Adleman (RSA), digital signature algorithm, Diffie–Hellman Algorithm key exchange, data encryption standard (DES), 3DES (Triple DES), advanced encryption standard (AES), Blowfish, and RC4 to name a few. All the algorithms provide a high level of CIA -- confidentiality, integrity, and authentication and on –and non-repudiation, which certifies that the sender cannot refute the authenticity and validity of the communication [62]. Digital signatures are also a method to confirm the authenticity of a sender's message without alterations. All data must be encrypted to protect the integrity of data at rest, motion, and or in transit. Most cyber exploits occur when information is in transit, while users are authenticated [63]. The importance of encryption ensures that hackers cannot decrypt stolen data.

3.3 Antivirus Software

The best measure against viruses is to install and update an antivirus program [64]. Sixty-eight percent of organizations have effectively incorporated comprehensive antivirus and antispyware programs, thus improving their security posture [65]. There are numerous antivirus programs widely used (Trend Micro, Norton, and McAfee Virus Scan). Antivirus software is already ready for trial use in most computers nowadays. The key is to continue upgrading the antivirus program to its latest version to comprise all new detectable signatures. Antivirus alone is not feasible to protect an environment from all types of cyber threats, and the use of additional components are necessary to strengthen its capabilities [66]. Antivirus programs can also check for spyware and are essential. Notable spyware programs currently available are CounterSpy, STOPzilla, Spyware Doctor, and Spy Sweeper. An ad-blocking feature must be installed in the web browser to protect against adware [64]. Antivirus and antispyware programs have features to also guard against software keystroke and loggers for additional protection. It is also important to reiterate the antivirus software is not enough against security threats alone [67]. Antivirus is notably less effective against cyber threats, and hackers are becoming extremely skilled at bypassing environmental security measures [66]. Cyberattacks are prevalent, and organizations must understand the overhaul of a specialized security tool is imperative. As an example, Kaspersky Endpoint Security for Business is a tailored solution to protect IT infrastructures against cyber threats [65].

3.4 IPDS

Defined security systems such as antiviruses, firewalls, and intrusion detection systems, IDS, are solutions to protect infrastructure against hackers and crackers. Most IDS are network-based and do not require definition updates for detection, unlike antivirus programs [68]. IDS functions analyze malware behaviors dynamically. There are also other means of detections, such as the signature-based detection to match observed predefined intrusive behaviors on the network [69]. This method is the simplest to integrate, but it is time-consuming to continually update its anomaly definitions. IDPS are necessary security measures to protect the network internally and externally [70]. IDPS uses three types of methodologies to detect offenses: signature-based, anomaly-based, and stateful protocol analysis [71]. Improper threat detection is a common issue within IDPS and leads to many false-positive alerts, buffer overflow, and SQL server attacks [70].

3.5 Firewalls

Firewalls share the same functionality as a router, in which filters are used to distinguish between valid and invalid data packets [72]. Firewalls are a combination of hardware and software vulnerable to misconfiguration and manipulation. The different types of firewalls are packet filtering, application and proxy, stateful, and next-generation firewall (NGFW). As previously stated, firewalls alone are not a failsafe solution. Along with IDPS, defence-in-depth IT security programs can further the ability to respond to threats more effectively. Employing the right set of rules and policies can reduce rising anomalies from passing through firewalls. Problems occur within a complex environment where traditional rules conflict with each other and dilute the intended security effectiveness [73]. When security tools such as IDPS accompany the use of proper firewall rule configurations, packets can be analyzed thoroughly.

4. Recommended Security Tools

Most interview participants state the importance of cybersecurity and continuous endeavors to apply current security tools and methods. Many organizations must implement firewalls, IDPS, encryption, SIEM, and antivirus software. Hackers are persistent and knowledgeable of systems with identified unknown that vulnerabilities (zero-day) to the cybersecurity community. Exploits are impacting organizations worldwide with increasing security breaches [4]. The cybersecurity professionals in this study provided a

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

significant amount of information regarding the direction for a stronger security environment. The following respondents provided extra information to shed light on technical securities they recommend within an organization. All respondents responded to known security tools such as risk tolerance, better physical security, least privilege, redundancy, monitoring, and education and training. Security professionals mentioned the use of the PAM-based detection (protocol analysis module) that is developed by IBM X-Force IRIS systems, the use of an air-gapping system, an AI (artificial intelligence) to include pattern, knowledge, algorithmic, or self-learning, a website security blockers to provide security protection [74], technical debt within software projects [75], and to adopt the cyber kill chain model for the identification and prevention of cyber intrusion activity to identify the steps cybercriminals must complete to exploit the system. Conversations with cybersecurity professionals reiterated the constant challenges of cyber threats that many organizations face [76]. Many aspects of security must be applied to mitigate cyberattacks by using SIEM, IDPS, training, innovations, and effective security policies. Also, there were a few points not discussed during the interviews concerning the furtherance of cybersecurity preparation. Endpoint security software is designed to enforce the organization's security objectives and report its statuses to the centralized management system for monitoring. The APT, or advanced persistent threat, is the most severe threat to security because of customized malware developed by APT actors [77].

Sandboxing is a method used to identify malicious software based on behavior rather than signature analysis. The purpose of the method is to isolate suspicious codes into a unique environment, or sandbox, to isolate from other systems and applications. IDPS and firewalls can detect scans and probes that are precursors for future security-focused attacks, such as DoS and DDoS, on the infrastructure. Upper management, such as the CEO, must reinforce the importance of cybersecurity within the organization. Also, the development of secure coding practices helps certify that the necessary controls are in place against any exploits [78]. The OSWAP – Open Web Application Security Project – provides proactive controls for web application security to encompass input validation, session management, access control, error handling, logging, data protection, and communication security, to state a few.

4.1 NIST Framework and ISO 27001 Standards

The NIST cybersecurity framework provides organization management processes based on Tiers implementation (Tier 1: Partial, Tier 2: Risk-Informed, Tier 3: Repeatable, and Tier 4: Adaptive) to help to improve an infrastructure's critical security posture [79]. The tool is intended to provide the organization with a baseline to measure its cybersecurity apparatus. The framework is also voluntary, unenforced by any authority, and organizations have the clear choice of developing their cybersecurity program. The distinction between internal and external failures is critical [80]. ISO 27001 includes security objectives covering 14 categories from encryption, information security policies, and incident management. The standard has a meaningful role but is not recommended as the single best security practice [81]. The application of various security practices together can strengthen the overall security platform.

5. Theories Implications

The exploratory research seeks to examine additional security tools to help organizations efficiently mitigate cyber threats. Analysis of the interviews shows the importance of using secure methods such as SIEM, PDS, firewalls, antivirus software, education, continuous training, and the services of ethical hackers to test security defenses. The human factor is the crucial element since insider threats account for more than 50% of all breaches [31][82]. The research findings correlate to what has already been established within the literature regarding the increasing importance of cybersecurity, and the severe challenges that cyberattacks pose for organizations. A theoretical framework such as the planned behavior (PBT), deterrence theory (DT), and protection motivation (PMT) have been the three fundamental theories of managing, promoting, and discouraging behaviors from avoiding catastrophic security events.

5.1 Planned Behavior Theory

Planned behavior theory (PBT) emphasizes behaviors via attitudes, subject norms, and perceived behavioral control [83]. People tend to behave in a specific manner because of emotional interests. PBT helps determine ethical conduct and appropriate actions against violated policies [84]. People must be kept interested, focused, and treated as of equal importance. Promoting positive employee motivation can discourage any potential unfortunate behavior. Because people change based on varying determinants, more studies are necessary to become more familiar and accurate with regards to behavioral conduct. The data also reveals the importance of more training and continuous education of employees. A previous study demonstrates that cybersecurity must be efficacious [85]. This idea is also applicable to individuals because the promotion of ethical behavior is ultimately beneficial to the organization. This study also shows that cybersecurity

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

professionals are applying current security tools and methods, along with additional security tools, to further the security of their environment.

5.2 Protection Motivation Theory

Protection motivation theory (PMT) focuses on empowering people to undertake actions that benefit their environment in what has been called "self-and-response efficacy" [40]. Like PBT, the theory encompasses "fear of appeal," and coping appraisal contributes to how much a person would deviate from acting against policies or norms [40]. Interview participants noted that people are the cause of many internal issues, but under the right plan and motivational culture, risks associated with insider threats could be significantly reduced [11]. The previous study indicated that PMT drives employees to voluntarily comply with internal procedures [86]. PMT yields positive results like compliance [11]. However, with the right management and motivation, the reinforcement of ethical values could be a significant competitive advantage. Previous studies found that further implementation of PMT could bridge the gap between good and bad behaviors [40].

5.3 Deterrence Theory

Lastly, deterrence theory (DT) shares similarities with PMT, where the organization could employ adequate repercussions to dissuade adverse actions [87]. Analysis of the completed interviews presents information related to the behavior and security controls of the workforce and organizational activities. Reducing individual infrastructure access is a factor. Planning, auditing, and enforcing security standards are essential. The emphasis on annual employee training and education is fundamental. Understanding that internal people are the source of breaches is a starting point. DT is a crucial factor to identify and eliminate undisciplined characters and mitigate risks by implementing the best security standards. The fear of prosecution and imprisonment resulting from breaching protocol can alter individuals' behavior [88]. Further research in information security is recommended to further develop DT [89]. Fear-based communication models could be an attribute within the information security model to promote the deterrence of lousy behavior [90].

6. FINDINGS

Cyber threats are phenomena with no boundaries. Digital thieves apply techniques to penetrate secured infrastructure at will with ease, sophistication, and patience. The essence of the problem starts with people. Whether from an internal or external perspective, individuals are the reason for internal misconfiguration, intentional sabotage, social engineering, and unethical hacking. Security applications could be compromised, but with the right combination of motivated, dedicated, and experienced individuals, this scenario could be avoided. The steps to threat confinement do not stop with employee training and education. Experienced cybersecurity professionals must stay abreast of all new security threats, such as ransomware, and be able to mitigate them. Also, internal protocols should be in place to restrict access and modification of data. The integrity, availability, and confidentiality of the assets must be monitored. Ultimately, security must apply a combination of multiple methods to safeguard data. The combination of the right people, technology, and policies provide the best advantage to prevent damaging incidents.

7. LIMITATIONS

Although cybersecurity is a hot topic, most organizations never communicate and share current and past intrusions unless they are part of a high-profile case [91]. The study followed the right to the participants as specified in the Belmont Report in 1979 to respect, protect, and perform the research based on the provided informed consent to everyone [92][93][94]. The result of the research remains anonymous as described in the consent form. The researcher maintained the validity and credibility of the study by keeping the records coded and held in a safe environment. The investigation does not permit further specific detailed information due to participants' need to maintain privacy about their organization's activities. Many possible participants declined to participate in the study based on their organization's internal policies preventing employees from discussing the security aspects of their respective company. Researching most organizations in the U.S. and analyzing their security posture and techniques would provide a wealth of information for future studies. Investigating the effect of cybersecurity and its relevant mitigation techniques is limited to only a fraction of the organization and may not reflect the action taken by most organizations.

8. IMPLICATIONS FOR PRACTICE

The findings in this research reveal the necessity for evolving cybersecurity, as well as the impact of cybercriminals on organizations' digital assets. Examining research concerning advanced methods for deterring cyber exploits is imperative. Emerging technologies such as the cloud, AI, behavioural analytics, and threat intelligence can work against the sophistication of future intricate cyberattacks. Standards such as ISO 27001/27002, NIST cybersecurity framework, COBIT, and ITIL can provide stronger security management processes. This research can guide

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

researchers to develop further security tools, and possibly incorporating new security program updates within the previously mentioned security standards. Future security developments can efficiently address emerging vulnerabilities by applying newly developed rules and keeping the infrastructure secure with the cybersecurity professionals' recommended techniques. The result of this study can guide future practitioners on how particular cybersecurity professionals address their security challenges with their respective organizations. Security professionals in the business, healthcare, and education industries can benefit by incorporation a more rigorous security apparatus. All professionals must understand the issue with security events not being investigated events. Those events can represent underlying hidden security risks in their environment. Too many organizations do not know a breach is occurring because the overall system does not correlate and identify the exploit correctly, and it is disregarded. Depending on the industry, the correct security measures must be applied to protect confidential information and intellectual property.

The investment in security is essential to incorporate the right tool as a complement to what is currently in place (Firewall, SIEM, antivirus, encryption, and IDPS). Security individuals must configure their security hardware and software to efficiently analyze all events and differentiate from ordinary to abnormal behaviours. This study did not identify how many security components any of the participant's organizations have in place but applying more than one security measure will improve the overall security risk the organization might face. Cybersecurity is crucial enough for all industries to incorporate the proper security measures. For example, software, site reliability, and hardware engineers must respectively test against security vulnerability before pushing for a software package update, SQL code injection, cross-site scripting, and vulnerabilities are built and configured correctly. This study considers the use of current security tools such as firewalls, SIEM, antivirus software, encryption, and IDPS to understand what additional security tools are used to reduce further, or defeat, the impact of cyber thieves and their attack sophistication. For instance, the results highlight the importance of continuous training, education, traffic monitoring, and behaviour analysis. Additional techniques such as the use of the IBM X-Force IRIS systems, AI, website security blockers, air-gapping systems, and technical debt can provide new strategies to confront cyber threats adequately.

9. Recommendations for Further Research

Further research leading to a greater understanding of security threats is necessary. The invasion of privacy caused by breaches is of constant concern. There must be a study to understand individual behaviour, both internally and externally, concerning organizations. Moreover, applying sets of controls to prohibit data theft is a requisite. The focus still should be concentrated on internal individuals and on how to comprehend their motivation using PMT and PBT on cognitive processes. The evaluation of continuous practical training and employee morale must be more in-depth. The effectiveness of organizational policies the impact on personal confidence is essential to investigate. More data must be made available to understand the state of an organization's security infrastructure and to rate its effectiveness using a scoring model and compare the results to other organizations successful in accurately determining their risk of failure. Reducing the gap between cybersecurity and cyber exploits is worth investigating by exploring frameworks such as ISO 17790/27001, ITIL, COBIT, and the NIST SP 800-53 and NIST SP 800-61, which are respectively the security and privacy controls for the Federal Information Systems and Organizations and the Computer Security Incident Handling Guide.

10. Ethical Consideration

The research upheld the intrinsic moral value, confidence, and respect without bias, personal beliefs, or prejudgments. The participants had the right to expect confidentiality and protection from the study. The data collection and the decoding of the information followed the guidelines of the research and IRB expectations in conducting the study. The researcher also educated himself on improving the correct interview procedures and expectations. Ethical training promotes a boost in morale and behaviour, as described in the literature, which is critical in the study [95]. The analyzed data using the qualitative software Atlas.ti was significant in recording, analyzing, and dissecting the results [96]. All interview responses were encrypted and kept confidential in case of loss or theft. It was crucial for the researcher not deviate from the research as described and specified in the provided consent form. All participants were not forced, controlled, coerced, or deceived per the guidelines and principles defined in this study expressed in the Belmont Report [93]. The researcher had the absolute obligation and duty to conduct the study concerning the values and expectations mentioned in the IRB process and to uphold accountability. Every aspect of the interviews followed the details provided in the consent form. All the objectives discussed and shared beforehand were articulated verbally and in writing to the respondents [97]. As described in the set of directives, safeguards were followed to conform to the ethical considerations in the qualitative study. Also, the researcher collected all approved permissions from participants and fully disclosed the data collection procedures. All information

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

the researcher collected was shared verbatim with the participants for transparency purposes. Individuals' right to privacy and anonymity were kept confidential as described and expected from the consent form. All aspects of the research protocol promoted a healthy protective environment as expected [98]. For the study to be reliable, all ethical concerns regarding the integrity, validity, and credibility of the research were answered and validated. Respectively, the participants' rights were preserved, and their identity was hidden. The integrity of the study was protected by following all processes detailed in the consent form, along with the researcher's demonstrated ethical behavior. The study acquired its validity because all vetted participants fulfilled the requirements. The credibility of the study was based on the result of each previous criterion to reinforce the purpose of the research. Hence, the risk of failure was eliminated and made the overall experiment more factual, sound, and credible.

11. Conclusions

Cyber threats are growing and are continuously impacting businesses and the economy worldwide. The literature reveals a theme in stopping cybercriminals from stealing data and compromising network systems with sophisticated attacks to affect the integrity, availability, and confidentiality of information. Because of increasing exploits, engaging cybersecurity professionals to analyze the scope of the problem is essential. The issue is that technology and innovation are growing, and so are the attack surfaces. Hackers always find unknown, new, and intricate vulnerabilities to exploits, which make it harder for security defenses to neutralize. The gap between cybersecurity and cyberattacks is growing, and improving defensive measures is vital. Cybersecurity professionals in the study highlighted focusing on people, training, education, configuration, and robust security policies. Implemented security tools and techniques such as SIEM, IDPS, and encryptions must be up-to-date and continually configured to adapt to new types of attack vectors.

It is imperative to understand the attack surface and to implement the right security apparatus at the right place with scope and budget. Related studies reveal gaps in communication and cooperation between organizations. Also, management involvement is critical and not just during the remediation and recovery process post-attack. The human factor, especially insider threats, must be evaluated. Insider attacks become malicious due to carelessness, lack of knowledge, or misconfiguration of security policies. Behavior analysis is essential: Using PMT, PBT, and DT on cognitive processes can help assess individual and technical perceptions. Security standards such as ISO 27001, ITIL, and the NIST cybersecurity framework can help organizations apply for the best-recommended security approaches and programs. The evaluation of continuous practical training and employee morale must be more in-depth. The effectiveness of policies within the organization and the impact on personal confidence is essential to investigate.

More data must be made available to assess the state of an organization's security infrastructure and to rate its effectiveness. Comparing results with other organizations successful in determining their risk of failure is a benefit. The invasion of privacy caused by breaches is a concern and must be investigated thoroughly and continuously. Future research exploring new security methods and techniques is essential. Cybercrime is a multifaceted issue; no single solution can eliminate the problem. Technology is always evolving, and advanced new applications and tools are developed worldwide to give businesses and regular users the ability to apply new techniques. Equally, hackers are learning and developing countermeasures to bypass security barriers. Enhancing security standards such as the ISO 27001, ITIL, and NIST can further the understanding and development of stricter security recommendations. Facilitating communication within organizations regarding current threats is also another area for further research.

References

[1] Sharma, M. P., Zawar, M. S., & Patil, S. B. (2016). Ransomware analysis: Internet of things (Iot) security issues, challenges and open problems in the context of worldwide scenario of security of systems and malware attacks. Int. J. Innov. Res. n Sci. Eng, 2(3), 177-184.

[2] Hewes, C. A. (2016). Threat and challenges of cyber-crime and the response. S.A.M. Advanced Management Journal, 81(2), 4-10, 2.

[3] Neal, P., & Ilsever, J. (2016). Protecting information: Active cyber defense for the business entity: A prerequisite corporate policy. Academy of Strategic Management Journal, 15(2), 15-35.

[4] Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. MIT Sloan Management Review, 58(3), 71-77.

[5] PWC, P. (2015). Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015.

[6] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135.

[7] Alnatheer, M. A. (2014). A conceptual model to understand information security culture. International Journal of Social Science and

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Humanity, 4, 104-107. Retrieved from http://www.ijssh.org/papers/327-A00013.pdf

[8] Gaigole, M. S., Kamaltai, S., & Kalyankar, M. A. (2015). The study of network security with its penetrating attacks and possible security mechanisms. Int. J. Comput. Sci. Mob. Comput, 45(5), 728–735.

[9] Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. Journal of the Association for Information Systems, 18(1), 22-44.

[10] Chowdappa, K. B., Lakshmi, S. S., & Kumar, P. P. (2014). Ethical hacking techniques with penetration testing. International Journal of Computer Science and Information Technologies, 5, 3389-3393. Retrieved from http://www.ijcsit.com/

[11] Siponen, M., Pahnila, S., & Mahmood, M. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224.

[12] Alazab, M., Venkatraman, S., Watters, P., & Alazab, M. (2011). Zero-day malware detection based on supervised learning algorithms of API call signatures. In Proceedings of the Ninth Australasian Data Mining Conference, 121, 171-182.

[13] Murshudli, F., & Loguinov, B. (2019). Digitalization Challenges to Global Banking Industry. Varazdin: Varazdin Development and Entrepreneurship Agency (VADEA).

[14] Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the Gap between Organizational Practices and Cyber Security Compliance: Can Cooperation Promote Compliance in Organizations? International Journal of Business & Society, 19(1).

[15] Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F., Jr. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. Journal of Management Information Systems, 34(4), 1023-1053.

[16] Emery, A. C. (2017). Zero-day responsibility: The benefits of a safe harbor for cybersecurity research. Jurimetrics, 57(4), 483-503.

[17] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.

[18] Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. International Management Review, 13(1), 37-58,101-102.

[19] Cohen, A. (2018). Effective Cyber Leadership: Avoiding the Tuna Fish Effect and Other Dangerous Assumptions. The Cyber Defense Review, 3, 47-52.

[20] Benson, V., McAlaney, J., & Frumkin, L. A. (2019). Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications, 1264-1269. doi:10.4018/978-1-5225-8897-9.ch062

[21] Karahan, S., Wu, H., & Armistead, L. (2019). Evolution of US Cybersecurity Strategy. In International Conference on Cyber Warfare and Security, 168-176. Academic Conferences International Limited.

[22] Parrend, P., Navarro, J., Guigou, F., Deruyver, A., & Collet, P. (2018). Foundations and applications of artificial intelligence for zero-day and multi-step attack detection. EURASIP Journal on Information Security, 2018(1), 1-21.

[23] Davis, A. (2012). Hacktivism. ITnow, 54(2), 30-31.

[24] Habeeb, R. A. A., Nasaruddin, F., Gani, A., Hashem, I. A. T., Ahmed, E., & Imran, M. (2018). Real-time big data processing for anomaly detection: A survey. International Journal of Information Management.

[25] Malecki, F. (2019). Best practices for preventing and recovering from a ransomware attack. Computer Fraud & Security, 2019, 8-10. ISSN 1361-3723. doi:10.1016/S1361-3723(19)30028-4

[26] Wolff, J., & Lehr, W. (2017). Degrees of Ignorance about the Costs of Data Breaches: What Policymakers Can and Can't Do about the Lack of Good Empirical Data. doi:10.2139/ssrn.2943867

[27] Gillon, K., Branz, L., Culnan, M. J., Dhillon, G., Hodgkinson, R., & MacWillson, A. (2011). Information Security and Privacy-Rethinking Governance Models. CAIS, 28, 33.

[28] Wolff, J., & Lehr, W. (2018). When cyber threats loom, what can states and local governments do? Georgetown Journal of International Affairs, 19, 67.

[29] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.

[30] Caravelli, J. (2019). Cyber Crime. Cyber Security: Threats and Responses for Government and Business, 23.

[31] Guozhu, M., Yang, L., Jie, Z., Pokluda, A., & Boutaba, R. (2015). Collaborative security: A survey and taxonomy. ACM Computing Surveys, 48(1), 1-42.

[32] Brief, K. (2017). Arbor Networks is recognized as the 2017 Market and Technology Leader in the Global DDoS Mitigation Market. Retrieved from https://pages.arbornetworks.com/rs/082-KNA-087/images/Knowledge%20Brief_Arbor%20Netw

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

orks_Market%20Technology%20Leader_DDoS%20Mitigation%20FINAL.pdf
[33] Mee, P., & Schuermann, T. (2018). How a cyberattack could cause the next financial crisis. Harvard Business School Publishing. Retrieved from https://hbr. org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis
[34] Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. Pew Research Center, 26.
[35] Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. Information System Frontiers, 15(1), 5-15.
[36] Chen, S., & Janeja, V. (2014). Human perspective to anomaly detection for cybersecurity. Journal of Intelligent Information Systems, 42, 133-153.
[37] Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, 447-459.
[38] Hua, J., & Bapna, S. (2013). Whom can we trust? The economic impact of insider threats. Journal of Global Information Technology Management, 16(4), 47-67.
[39] Barrios, R. (2013). A multi-leveled approach to intrusion detection and the insider threat. Journal of Information Security, 4, 54-65. doi:10.4236/jis.2013.41007
[40] Hsu, J. S. C., & Shih, S. P. (2015). When does One Weight Threats more? An Integration of Regulatory Focus Theory and Protection Motivation Theory. Retrieved from http://aisel.aisnet.org/wisp2015/12
[41] Floyd, D. L., Prentice-Dunn, S., & Albery Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407-429.
[42] Shane, S., Perlroth, N., & Sanger, D. E. (2017). Security breach and spilled secrets have shaken the NSA to its core. The New York Times. Retrieved from https://cyber-peace.org/wp-content/uploads/2017/11/Security-Breach-and-Spilled-Secrets-Have-Shaken-the-N.S.A.pdf
[43] Computer Fraud & Security (2019). New reports reveal scale of nation-state hacking, 2019(3), 1-3. ISSN 1361-3723. Doi:10.1016/S1361-3723(19)30023-5
[44] Thomas, G., Burmeister, O., & Low, G. (2018). Issues of Implied Trust in Ethical Hacking. ORBIT Journal, 2(1).
[45] Identity Theft Resource Center (2017). 2017 annual data breach year-end review. Identity Theft Resource Center: California.
[46] Emerson, R. G. (2016). Limits to a cyber-threat. Contemporary Politics, 22, 178-196. doi:10.1080/13569775.2016.1153284
[47] Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality—An empirical study. Accounting and Management Information Systems, 15(1), 112-130.
[48] Zabicki, R., & Ellis, S. R. (2017). Penetration Testing. In Computer and Information Security Handbook, 1031-1038. doi:10.1016/B978-0-12-803843-7.00075-2
[49] Branquinho, M. A. (2018). Ransomware in industrial control systems. What comes after Wanacry and Petya global attacks? WIT Transactions on the Built Environment, 174, 329-334.
[50] Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2019). Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures. arXiv preprint arXiv:1901.03899.
[51] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113-122.
[52] Nhan, J. (2014). Phishing. In C. J. Forsyth, & H. Copes (Eds.), Encyclopedia of social deviance.: SAGE Publications: Thousand Oaks, CA.
[53] Zhao, M., An, B., & Kiekintveld, C. (2016). Optimizing personalized email filtering thresholds to mitigate sequential spear phishing attacks, 658-665.
[54] Enigbokan, O. K., & Ajayi, N. (2017). Managing cybercrimes through the implementation of Security measures. Journal of Information Warfare, 16(1), 112-129.
[55] Rassam, M. A., Maarof, M., & Zainal, A. (2017). Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges, and Trends. Journal of Information Assurance & Security, 12(4).
[56] Elngar, A., Mohamed, D., & Ghaleb, F. (2012). A fast accurate network intrusion detection system. International Journal of Computer Science and Information Security, 10(9), 29-35.
[57] El-Taj, H., Najjar, F., Alsenawi, H., & Najjar, M. (2012). Intrusion detection and prevention response based on signature-based and anomaly-based: Investigation study. International Journal of Computer Science and Information Security, 10(6), 50-56.
[58] Genç, Z. A., Lenzini, G., & Ryan, P. (2017). The Cipher, the Random and the Ransom: A Survey on Current and Future Ransomware. Advances in Cybersecurity 2017. Retrieved from http://hdl.handle.net/10993/32574
[59] CISCO. (2017). Annual Cybersecurity Report.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[60] Bjorke, J. D., & May, J. D. (2016). Trends in recent data breach litigation. Franklin Business & Law Journal, 2016(4), 52-66.
[61] Leonard, S. M. (2013). Cybercrime. In C. G. Bates, & J. Ciment (Eds.), Global social issues: An encyclopedia. Routledge: London, UK.
[62] Singh, P. K., & Chandel, G. S. (2014). A modified technique for performing data encryption & data decryption. International Journal of Engineering Research and Applications, 4(7), 149-152.
[63] Mahbod, R., & Irish, R. (2017). A Guide to Cybersecurity. The Journal of Government Financial Management, 66(3), 34-39.
[64] Bidgoli, H. (2016). Integrating real-life cases into a security system: Seven checklists for managers. American Journal of Management, 16(4), 9-25. Retrieved from http://www.m.www.na-businesspress.com/AJM/BidgoliH_Web16_4_.pdf
[65] Iovan, S., & Iovan, A. (2016). From cyber threats to cyber-crime. Journal of Information Systems & Operations Management, 425-434.
[66] Birtstone, R. (2015). Don't count on antivirus software alone to keep your data safe. Available online at http://www.theregister.co.uk/2015/02/09/dont_ count_on _antivirus_alone_to _protect_your_data/
[67} Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality—An empirical study. Accounting and Management Information Systems, 15(1), 112-130.
[68] Singh, R., Kumar, H., Singla, R .K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system. Online Information Review, 41(2), 171-184.
[69] Elshoush, H. T., & Osman, I. M. (2011). Alert correlation in collaborative intelligent intrusion detection systems—A survey. Applied Soft Computing, 11, 4349-4365. doi:10.1016/j.asoc.2010.12.004
[70] Rizvi, S., Labrador, G., Guyan, M., & Savan, J. (2016). Advocating for hybrid intrusion detection prevention system and framework improvement. Procedia Computer Science, (95)1, 369-374.
[71] Turner, C., Jeremiah, R., Richards, D., & Joseph, A. (2016). A rule status monitoring algorithm for rule-based intrusion detection and prevention systems. Procedia Computer Science, 95(1), 361-368.
[72] Firstenberg, M. (2017). Industrial cybersecurity: How much is enough? Chemical Engineering Progress, 113(6), 26-29.
[73] Guri, M., & Elovici, Y. (2018). Bridgeware: The air-gap malware. Communications of the ACM, 61(4), 74-82.
[74} Marotta, V., & Acquisti, A. (2017). Online distractions, website blockers, and economic productivity: A randomized field experiment. Preliminary Draft.
[75] Alves, N. S., Mendes, T. S., de Mendonça, M. G., Spínola, R. O., Shull, F., & Seaman, C. (2016). Identification and management of technical debt: A systematic mapping study. Information and Software Technology, 70, 100-121. doi: 10.1016/j.infsof.2015.10.008
[76] Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: Challenges and opportunities. Cyber Threat Intelligence, 1-6.
[77] Lv, K., Chen, Y., & Hu, C. (2019). Dynamic Defense Strategy against Advanced Persistent Threat under Heterogeneous Networks. Information Fusion.
[78] Gupta, S., & Gupta, B. B. (2017). Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges. International Journal of Cloud Applications and Computing (IJCAC), 7(3), 1-43.
[79] Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. Journal of Internet Law, 18(6), 3–6.
[80] Radziwill, N., & Benton, M. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. Software Quality Professional, 19(4), 25-43.
[81] Brown, W., & Nasuti, F. (2005). What ERP systems can tell us about Sarbanes-Oxley. Information Management & Computer Security, 13, 311-327.
[82] Loukaka, A., & Rahman, S. (2017). Discovering new cyber protection approaches from a security professional prospective. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *9*.
[83] Zolait, A. S. (2014). The nature and components of perceived behavioral control as an element of theory of planned behavior. Behaviour & Information Technology, 33(1), 65-84.
[84] Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security, 23(2), 200-217.
[85] Sharma, A., & Misra, P. K. (2017). Aspects of enhancing security in software development life cycle. Advances in Computational Sciences and Technology, 10(2), 203-210.
[86] Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3), 190-198.
[87] Deterrence theory. (2015). In J. Mcray (Ed.), Leadership glossary: Essential terms for the 21st century. Santa Barbara, CA: Mission Bell Media.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[88] Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly, 37(1).
[89] Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90-101.
[90] Posey, C., Roberts, T., Lowry, P. B., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. Mis Quarterly, 37(4), 1189-1210.
[91] Muegge, S., & Craigen, D. (2015). A design science approach to constructing critical infrastructure and communicating cybersecurity risks. Technology Innovation Management Review, 5(6), 6-16.
[92] Corman, J. (2010). Principles of ethical review. Applied Clinical Trials, 19(7), 2-8A, 9A.
[93] Department of Health, E. (2014). The Belmont report. Ethical principles and guidelines for the protection of human subjects of research. The Journal of the American College of Dentists, 81(3), 4.
[94] Hoser, B., & Nitschke, T. (2010). Questions on ethics for research in the virtually connected world. Social Networks, 32(3), 180-186. doi:10.1016/j.socnet.2009.11.003
[95] Yazdani, N., & Murad, H. S. (2015). Toward an ethical theory of organizing. Journal of Business Ethics, 127, 399-417. doi:10.1007/s10551-014-2049-3
[96] Ilvonen, I. (2013). Information security assessment of SMEs as coursework—Learning information security management by doing. Journal of Information Systems Education, 24(1), 53-61.
[97] Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approach. Sage publications.
[98] Jackson, D. (2013). What are qualitative research ethics? Journal of Research Administration, 44(1), 93-95.

Authors

Dr. Alain Loukaka: Dr. Alain Loukaka received his degree in the Information Security and Information Assurance program at Capella University, Minneapolis, USA. Alain's exploratory research was on cybersecurity exploits and advanced methods of detection beyond current know applications. Alain has a Masters' in Information Technology from Florida Tech and a BS in IT Networking with a security emphasis from Clayton State College and University. Alain has been in the IT field for more than 15 years and plans to use his work to promote better security approaches and deterrents.

Dr. Shawon Rahman: Dr. Shawon S. M. Rahman is an Associate Professor in the Department of Computer Science at the University of Hawaii-Hilo, Hawaii, USA. Dr. Rahman's research interests include Information Assurance and Security, Digital Forensics, Software Engineering Education, Software Testing & QA, Cloud Computing, Mobile Application Development, and Web Accessibility. He has published over 120 peer-reviewed articles and is a member of many professional organizations including IEEE, ACM, ASEE, ASQ, ISACA, ISCA, and UPE.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731