DISCOVERING NEW CYBER PROTECTION APPROACHES FROM A SECURITY PROFESSIONAL PROSPECTIVE

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

[1]Ph.D. Candidate,Information Security Assurance,
Capella University, Minneapolis, MN, USA

[2]Associate Professor, Department of Computer Science
Majmaah University, Majmaah, Kingdom of Saudi Arabia

ABSTRACT

Cybersecurity has become a very hot topic due to high profile breaches that occurred in the past years. Despite the implementation of current known pre-emptive methods such as intrusion detection systems, anti-viruses, and the use of firewalls, hackers still find sophisticated means to steal data or impair an organization by targeting their assets. It is important that security professionals need to "think outside the box" and use new tools and techniques to mitigate threats beyond current known detections and prevention technologies. It is imperative that our infrastructure and assets are impermeable from domestic and foreign attackers. Our best line of defense is the detection of any threats or vulnerability to prevent or minimize damages of our assets from domestic and foreign attackers.

KEYWORDS

Cybersecurity; Information Security; Intrusion Detection; Information Systems;Vulnerability; Security Professional; Exploits.

1. INTRODUCTION

Information security is a crucial topic to address and to implement within any organizations to ensure the safeguards of their internal assets and intellectual properties[1]. Most organizations do conduct business via the cyberspace which has become more convenient and provided real time connection and communication especially for users[2]. The use of such technology has provided an opportunity for hackers to penetrate companies' infrastructure and to exploit their vulnerabilities [3]. Cyber security has become an important subject to address malice used by malevolent users to steal information[4]. Cyber security attacks are performed by individuals or groups for criminal or personal purposes that usually include financial motivations[5]. Increased cyber attacks are due to attackers being more sophisticated in this ever evolving and complexed digital economy that has grown exponentially[7]. Exploits have increased tremendously in the past decade which resulted in the increase or property loss, privacy, data theft, which impacted consumer confidence[8]. Exploits increased more than 42% by 2012 with an average of 116 targeted incidents daily[11]. According to the Federal Bureau of Investigation (FBI), infected systems with ransom ware generated more than $209,000,000 in early 2016 and increasing attacks are more prevalent[14]. In that instance, 32% of surveyed executives stated that investment in security will be a priority in 2017 compared to 2015[16].According to the Threat Stats report, 91% of attacks starts with email[18].

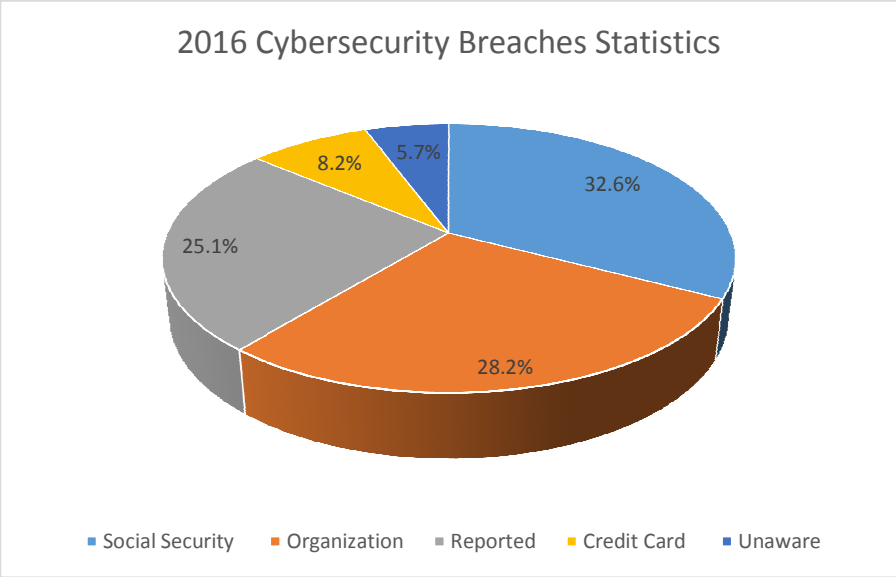

Fig. 1. Cyber security breaches in 2016 in the United States. Data from Threat Stats, *SC Magazine: For IT Security Professionals (15476693)*, *28*(2), 6-7.

In order to detect attacks more accurately and to build on a robust detection system, it is imperative to apply other areas that include new technologies, big data, attacker philosophies and the normal user activities[21]. Understanding how businesses compile and manipulate data is needed in future studies to comprehend what might contribute to security failure and analyzing their ethical processes[26]. The question is how intrusion detection systems tools and configurations can be further implemented to better deal with cybercrimes to mitigate accruing theft and financial loss from security professionals' prospective[71].

2. INTRUSION DETECTION PROBLEMS

In order to efficiently improve the security of organizations and to mitigate the rise of exploits, it is important to focus on the Intrusion Detection Systems (IDS) that is used and employed, or should be employed, by most organizations to ultimately safeguard their data[71]. It is fundamental to have IDS be familiar with any new attacks that hackers use to access systems and to be able to launch suitable countermeasures against such ill activities[13][36]. Protecting the network rests on the fundamental importance that intrusion anomaly rests on IDS to effectively identify and destroy any types of malicious activities from damaging the system and accessing valuable information. IDS are an important tool because its implementation will help detect anomaly behaviors and apply detection mechanisms to possibly detect unauthorized access or/and behavior that can compromise the system[71]. One important factor is that there is a significant gap in the literature when it comes to information security management[38]. Organizations need to understand how to identify the threats they may be facing and how their data need constant protection[1]. Implementing tools and techniques to ensure the integrity, availability, confidentiality, and accountability of the system are essential to the survival of the organization[59]. Observing such activities is crucial in identifying accurate attacks especially when it comes to false negative and positive alerts [34][21]. Researchers have analyzed and debated about the anomaly detection dilemma and concluded that alternatives have been elusive. Again, with advanced stealth methods from attackers, it has become a very complexed procedure to identify and systematically difficult to address every malicious intrusion in systems[21].

3. BACKGROUND STUDY

3.1 RESEARCH

Because of very little research in this area, proposed data protection mechanisms have been scarce in detecting such abuse from internal users when they utilize their system privilege to violate the organization security procedures and the handling of data[78]. The impact of internal misuse of information within the organization has increased the vulnerability and risks associated with such abuse[44]. A useful strategy is to implement different security concepts to deter any possible internal threats such as employing disciplinary actions to control human behavior and attitude, the use of more monitoring surveillance, perimeter defense, and notably incorporating decoys as a mean of deception to attackers[8].

In contrast, looking at what is needed to ameliorate the status quo in regards to enhancing IDS, it is not hard to see that there is a long battle ahead to overcome security threats internal and external. As stated previously, developing systems that are absolutely exploit free is very difficult and close to impossible in the positive and negative IDS alerts[17]. And this become a greater endeavor because regardless of what procedures are in place, an organization is still at risk not only from external attacks but also from the ones from within[35]. Such gap is a representation of what literature has shown because no concrete research to alleviate and understand how to reconcile this security management dilemma has been made[38]. In one hand, it is important to deter security exploits from external sources but at the same time deter exploits from your own organization.

3.2 APPLIED METHODS

Again, job rotation, separation of duties, and vacation time are not enough to prevent malfeasance [45]. The principle of least privilege does not prevent access rights that are accurately allowed. Nowadays, organizations cannot always restrict minimal access for employees due to their business demands[75]. Thus the need for collaboration is needed to bridge the gap between efficient IDS and insider and outsider threats[9]. As long as this gap exists, it will be very difficult to understand and mitigate most of the security holes that expose infrastructure information to hackers[38].

The insider threat is not only costly but was hard to detect especially when the person is already part of the organization[37]. Now, at any given time, an organization needs to focus on two fronts to mitigate unknown attacks. It is possible to study patterns and attributes of certain or all events but if the end focus is not determine, it could lead in missing exploits unless IDS detected it as being an anomaly[23]. Some research refer to this dilemma as the “Dark Side of IT” where stopping an employee that has access to sensitive information is difficult if he/she wants to sell to competitors but implementing strong security policy is critical in such situation[73]. The insider threat does not seem to have a concrete resolution due to people uncertain conduct[45]. It is difficult to integrate great security measures because organizations may need to grant higher access to certain employees, make sure the network is managed accurately and that all personnel activities are monitored, and that they adhere to company security and ethical policies[35].

4. ETHICAL BEHAVIOR

Addressing ethical issues related to practices, policies, and confidentiality would bridge the gap between security and risk management in organizations to help mitigate the increase in infrastructure exploits due to poor system design[24]. Understanding the mechanism and how organizations operate, ethical issues can arise and decisions will need to be made at the

management level to address such concerns[9]. And compiling data that is needed in future studies will help comprehend what might contribute to security failure and analyze ethical processes[26]. Today's network infrastructure are so complexed that it is categorically impossible to adequately distinguish plausible valid alerts[21]. The literature does show that systems have flaws and that those very systems are hard to replace, ineffective, and vulnerable to increasing and sophisticated attacks from outside and especially inside[53]. IDS need to be adequately configured to perform as expected[13]. However, it does not mean that the security monitoring stops there. Security professional need to inspect and monitor all activities to be sure that all transmission are valid or not[21]. Because there is a significant gap in the literature, researching such phenomenon would be beneficial for all organizations[38]. Further research is needed to explain this phenomenon and to incorporate it as part of an information assurance strategy [1].The gap in the literature regarding information security management in organization is indeed significant[38]. Information technology has brought convenience to authorized and malicious users in terms of using the system to their advantage[2]. Cyber Security threats to the United States information systems infrastructure have increased and need to be constantly and effectively addressed[1].

5. INFORMATION SYSTEM THEORIES

There are three theories that can be implemented within information security. Those theories are the Theory of Planned Behavior (PBT), Deterrence Theory (DT), and Protection Motivation Theory (PMT). Those three theories can be integrated within the proposed dissertation topic by providing a better understanding of the phenomenon.

5.1 PLANNED BEHAVIOR THEORY (PBT)

Organizations need information systems and have to implement strong security measures to mitigate security threats[54]. Employees in an organization can become a potential threat intentionally or not[69]. Due to technology, current organizations depend on information systems to manage their data infrastructure. Beside using firewalls, anti-virus, backup, access control, and other security protocols, employees more than likely bypass security measures to complete a task[48]. The literature proposes the employment of security policies, education, training, awareness, and programs[6]. Studying additional factors that impact the employees' behavior can be useful[54]. Again communications within the organization regarding security policies need to be adequate and understood[69]. More than 50% of all breaches are caused by policy violations by employees[69]. PBT is a good predicting theory to approximate behaviors related to information security policy compliance[39]. PBT indicates that people are influenced by attitude based by norms and behavior control[69]. Previous research that have utilized the PMT noticed that anticipating employees' behavior was useful and critical[48]. It is also correct that such employees are the main reasons for information security to fail or prosper[48]. Future research in the qualitative area by doing interviews could add more substance to such research field[54]. Employees need to be aware of the consequences when it comes to security violation[69].

5.2 DETERRENCE THEORY (DT)

When it comes to human behavior, possible illicit activities can be controlled when severe punishment are in place[29]. Again, when it comes to internal defense, internal employees are still viewed as the weakest link regarding exploits and system mismanagement[27]. Significant advances in attack detection and prevention still do not protect against this type of vulnerability. Most of computers incidents are related to internal actions from authorized users[57]. Despite incorporation effective and necessary security measures, organizations are hit with exploits due to inappropriate actions[29]. The deviant behavior of insider threats whether malicious or accidental

are still prevalent and DT can be an additional layer to make aware that provisioned actions are in place against such occurrence[77]. When there is a strong severity in sanctions, deterrence control is highly affective[22]. It surely resonate in an employee's mind when it comes to violations intention[22]. Expectations from significant others do have a huge impact on potential violators[22].

Organizations should aim at deterring motivated or unmotivated users to think twice about their actions and to make sure they follow security policies[57]. Upper management should understand the priority in applying deterrence in security[29]. As an example, the ISO/IEC 27002 Standard for information security management infer to the deterrence theory when recommending guidelines[29]. Future research to include other means of control measures would be helpful. It is important to develop further perspectives theories to enrich the DT[22]. Further information security research would emphasize on the malicious or accidental behaviors to match them to their respective motivational trigger[27]. Fear based communication models have been used in recent studies using PMT within the behavioral information security domains[61].

5.3 PROTECTION MOTIVATION THEORY (PMT)

PMT elaborates on the fact that people would consider if they can take actions (self-efficacy) and if those actions will render the specific corresponding outcome (response efficacy)[43]. Organization are facing tremendous security issues from employees not conforming to internal security policies[67]. The organization needs to assure that their computer systems and its peripherals are compromised free[43]. Studies show that the internal threats are real and have potential negative influence[30]. Insiders' behavior accounted for almost half of the breaches[61]. Protecting the organization resource is imperative especially applying corresponding security measures[61]. Employees disdain for security policies compliance is a huge issue for organization[76]. Such behavior lead to security threats which account for half of all breaches[67]. Employees are more likely to comply with security specific policies or measures when they know what the end result[52]. Employees' attitude toward following precise security policies leads to actual policy compliance[67]. PMT does indicate how individual respond to the compliance stimulus and the motivation behind it and to deter them from malicious activities[76]. PMT has two factors that are perceived vulnerability and perceived severity and both factors do make employees believe positively when it comes to following security policies[67]. To reinforce the cognitive theory described in PMT, future compliance can be determined by bridging the gap between past employee behaviors to address future ones[76]. PMT helps determining the adherence to such policies by making policies convenient and part of a rewarding task[76].

6. IDS PROBLEMS

IDS do have three areas of interests that most researchers do address to highlight the problem that impair the reliability and effectiveness of detecting harmful actions and to help raise the correct alert[17]. Investigating IDS to mitigate the increase of computer crimes will be effective to reduce loss due to theft and help maintaining the integrity of personal and financial data[14][56]. IDS do have advantages and disadvantages that relate to the effectiveness of its functionalities and its abilities to perform successfully to prevent and thwart current and future attacks[12]. There are known problems that identify and emphasize on those issues by analyzing existing systems with known flaws because they cannot be easily replaced, the difficulty of developing secured systems, and understanding that those so-called secured systems are still vulnerable to inside malicious activities including human errors[35].

6.1 CURRENT SYSTEM FLAWS

First, addressing the issue with current systems that have flaws is crucial to determine how to bring them up to date and increase their efficiencies. The main overall problem revolve on organization being proactive after the attack occurred which I usually too late and detrimental. Too many companies really do not have any idea that they are being breached until after the fact. Hence, it is very important to proactively predict the emerging attacks by using some forms of analytics to build specific responses to appropriate exploits. Securing the organization assets is a great difficult task to tackle[72]. Because of the rise of identity thefts in the United States, cybercrime has become dominantly and unequivocally identified as a criminal act[53]. The implementation of IDS presents an important factor when it comes to anomaly detection which can potentially harm the system if not well defined and configured to effectively allow authorized access and behaviors[71]. Failure to detect valid anomalies can be fully ineffective in detecting any type of attack behavior and to pinpoint its sources which would make preventive actions ineffective[81]. As security has become an afterthought in most organizations, most failures are caused by the inappropriate detection methods to protect assets and consequently inadequate robust anti-penetration systems[24]. Corporate management have now been paying more attention to this phenomenon and have increased their interests in corporate security[63]. Formulating a solution has been a long debate when it comes to cyber threats. In 2016, a US legislation was introduced to promote information sharing and emphasizing on new standards to facilitate such endeavors via the NST, the U.S. National Institute of Standards and Technology. According to the Compound Annual Growth Rate (CGR), Cybersecurity attacks are on the rise and incredibly from 66% every year since 2009[20].With vulnerabilities that are designed flawed along with defects, hackers are able to infiltrate network and gain access to data and are able to control critical systems and proliferate denial of service.

Thus, flawed systems allow hackers to easily enter and navigate the network without being noticed due to ineffective internal security protocols[23]. Behavioral detection has become highly complexed due to the sophisticated attacks[7]. Protecting the confidentiality, integrity, and availability (CIA) of information are crucial since all security incidents are related to the manipulation of those three data elements[33]. Encryption does offer a greater sense of security for user stored data across the network but it also has brought questions and controversies when it comes to encrypting devices by default especially during an investigation where perpetrator data is locked safely[25]. There are many theories on how to improve IDS deficiency when it comes to anomaly detection to allow the alert management to help investigate logical patterns among incidents[60]. For instance, legitimate activities are not correctly detected by IDS and anomalies are referred as valid activities[17]. However, the disadvantage lies in false alarms due to authorized users and their behaviors causing the misidentification due to misconfigurations of the system[21]. Anomaly detection works by analyzing the historical data by detecting irregularities that differ from usual conditions[17].

Furthermore, using robust IDS would help detect attacks more accurately and by that utilizing studies from different areas, attacker psychologies, including new technologies, data mining skills, and the normal user behaviors[21]. Literature also highlights that there is a lack of information sharing between organizations relating to sensitive data breaches[51]. Organizations must understand the threats facing their information systems with direct impact on their business[21]. There is much to gain when security information regarding threats, systems vulnerabilities, and fixes for such system vulnerabilities are shared[74].

There is a great need to implement stronger security measures to address current challenges[1]. It is imperative to make sure that supportive measures are secured and corrective actions are applied[62]. Recent literature has only predominately focused on military and law enforcement

organization using defensive countermeasures[32]. Because of the shift in focus, there was no information on how to deal with private organizations and how to address holistic response measures[55]. And this is why threats increased because reliable information on the risk management of cyberattacks of critical infrastructures were not readily available[28]. Research to describe how cyber security measures need to be further addressed is necessary[66].

6.2 SECURED SYSTEM DEVELOPMENT

Secondly, there is an apparent difficulty in developing and implementing secured systems. It is understood and expected that all aspects of the infrastructure are protected from any kind of breaches that would target and affect the security, integrity, availability, confidentiality of the organization stored data[59]. When analyzing IDS, its configuration may impair the detection of harmful actions[17]. It is a categorical and legitimate problem for a system to distinguish between harmful and genuine behaviors[36]. The organization senior management team needs to utilize the fundamental of IT governance to define management directives, processes, and controls to assure that the information created, processed, stored by the organization, protected, and that rigorous information security practices are implemented[1].

Data theft and manipulation are the results of failed security implementations that allow attackers to commit criminal activities by targeting such permeable infrastructure. This created the phenomenon known as “advanced persistent threats” that are a well-groomed and resourceful adversaries backed by powerful government or groups[40]. The explosion of big data helped industries capitalize on financial and personal information such as credit cards and personal security details like social security number and so forth[51]. Information technology has offered great convenience to valid and unauthorized users[2]. As an example, web applications are essential tools for e-commerce and e-banking for they require the transmission of information required for payment[10][12]. Hackers gained profitable and unlawful profits in retrieving such communication medium for obvious and malicious financial reasons in most cases[12]. There is still a disconnection in the research community to propose a more elaborated IDS to tackle its failed properties[49].

Also, collaborations between organizations regarding security systems are necessary and better security will always prevail from serious disasters[9]. Cybercrime has become a growing and more sophisticated techniques that target the exploitation of systems worldwide[42]. All plausible scenarios need to be developed and formulated toward avoiding misidentified alerts[21]. It is also fundamental to keep in mind that the human element is a factor where system administrators need to analyze and improve practices to enhance IDS[68]. There is a great deal of opportunity to handle all the big challenges when it comes to better system definition and all associations to implement the right controls[13]. Some systems do currently use a static corresponding matching to decide what is best to deal with current penetration attempts[65]. The use of more methods are appropriate because intrusion patterns are complexed and evolving but could be predicted[21]. Implementing the right system response is more feasible compared to no appropriate protection at all[50].

In addition, well trained system analysts should be required monitor the system as well[59]. Hackers understand that the golden egg resides in the financial benefit of gaining access to those vulnerable infrastructure and data[50]. Regardless of current techniques that entail log analysis, packet filtering, and behavior analysis, it seems that some attacks still fall through the cracks[7]. Again, sophisticated and collaborated attacks against the organization should not just rely on one IDS aspect but all possible configurations to analyze and to recognize any abnormal activities[58]. A phenomenology approach would appropriately focus on the experiences of security professionals as a way to understand the issue openly and in depth[32]. The purpose of this research will be to describe how cyber security measures needs to be further addressed[66].

6.3 Insider and Outsider Threats

Last, understanding that secured systems are still vulnerable to inside malicious activities and/or human errors is important[35]. Basic executions can alleviate the vulnerabilities caused by human errors, weak implementations, and the lack of standard to thwart exploits especially in system life cycle[70]. One aspect of IDS that most organizations do not focus upon more consistently, compared to outside threats, is the inside threats[14]. IDS not only rest with former disgruntled employees but also programmers that do have a backdoor access to your network[14]. In fact, there is a big challenge on how to distinguish the insider threats from the cybersecurity threats because of the activity and digital signatures they produced[45]. When a hacker has access to a compromised system, authentication and authorization alone are not enough to prevent unauthorized access[14]. The insider threat has to become more addressed because it poses challenges when it comes to protecting the system especially database access[58]. Analyzing human behavior is not accurate and close to impossible and therefore techniques such as job rotation, vacation time, and separation of duties are tool to manage people and system effectively[45]. Unfortunately, people do crimes of opportunity such as sabotage, intellectual property theft, and fraud[19]. It is clear that any member of the organization dealing and having access to sensitive information still can perform incorrect or malicious system activities such as updates and misconfigurations[19].

Nonetheless, no major suitable solutions have been made to successfully approach the insider problem to adequately solve it[45]. Damaging effects on the reputation and consumers trust are a result of poor network assessment and management which affect the appropriate utilization of IDS[80]. And this is the biggest threats to organizations when security incidents emerge from internal sources[44]. The cause for not finding a reasonable solution for insider threats is because human behavior cannot be accounted for and the motive for performing such attacks varies[31]. The reasons could be related to being a hacktivist, spy (espionage), or just a government body eager to steal secrets[41]. When it comes to insider threats pre-emptive actions, it is important to identify the critical area that needs to be protected, have controls in place to eliminate future malicious activities, perform employees' awareness trainings, beware of terminated and disgruntled employees, and also incorporate some type of insider threats program that would help identify warning signs and questionable behaviors[64]. Insider threats are the most difficult security exploits that can be detected with an IDS because it does not account for such behavior[46].

7. IDS ISSUES AND THEORIES INTEGRATION CORRELATION

Hence, it was clear that those theories did align and did impact on the previous denoted IDS current known identified problems. For instance, when looking at the current system flaws, the PBT indicates that people in the organization are influenced by norms and behavior control. An organization management needs to understand what security protocols and policies are needed to enhance their current system status to better protect their assets. Such behavior is needed from top down so employees can benefit from it and understand the ideas behind it. The Deterrence theory does correlates with the secured system development needs because data should be protected from malicious access and the application of deterrent would be notified internal or external culprit that harsh punishment will be imposed on such offenders. As for PMT, most breaches are caused by some actions from the internal users. Employees' compliance to security policies is critical. Also, communicating to personnel that engaging in proper practices would help to prevent unforeseen situation from becoming worse.

7.1 THEORIES IMPLICATION

Based on the Planned Behavior, Deterrence, and Protection Motivation theories, it is important to incorporate policies to convey roper information to employees. It is imperative that upper

management also supports employees when it comes to policy application. In fact, the two bodies need to have an open communication channel to make sure that the company directives are well understood. Hence, promoting the need for internal staffs to do the right job and to comprehend the repercussions of some actions are essential. Because workers are part of the infrastructure, they can be the source of the problem but also can part of a pertinent solution. As the literature as shown, further research and considerations in behavioral analysis when it comes to information systems are necessary in order to further the understanding of why people do what they do and their motivation behind it.

7.2 ETHICAL CONSIDERATIONS

Ethical practices would help establishing a sound work environment. Employees need to feel that the task there are accomplishing would result in a positive outcome. It is also important for those users to understand that despite deterrent mechanisms in place that they are free from punishment by conducting themselves with respect and discipline. When members of the organization feel that they have some control, they will have the tendency to behave professionally with respect to their specific duties. Also, the literature shows that conducting ethical training does boost morale and consequently behavior[79].

8. CONCLUSION

A phenomenology approach would be beneficial to add to the body of language by having a depth conversation with security professionals and their take on the effectiveness of intrusion detection and the role of management[32]. Such conversation would highlight the issue on improper alerts that may render the system ineffective when the organization is subject to a sophisticated stealth attack[34]. The issue where activities are valid and identified as invalid needs to be addressed[60]. Research also shows that there is an economic impact after an attack but it also underlines that most organizations reluctance to change, adaptation, and collaboration[9]. Management needs to decide how much investment is good to provide adequate security which is usually an afterthought[3]. Most of all, there is no sign of collaborations between industries to exchange information regarding exploits as to what, where, and how hackers target, attack, and exploit a system in relation to a specific pattern[78]. Due to technology advancement and more complexed attacks, detecting intrusion detection has become more elusive[21]. Thus, in cybersecurity, intrusion detection is one of the needed area of research to be exploited. It is a great opportunity to increase and enhance our infrastructure to combat and stop current and potential exploits[1].

REFERENCES

[1].McFadzean, E., Ezingeard, J., & Birchall, D. (2011). Information Assurance and Corporate Strategy: A Delphi Study of Choices, Challenges, and Developments for the Future. Information Systems Management, 28(2), 102-129.

[2]. Ruey-Shin, C., Yu-Ming, C., & Tsai, C. (2010). A study of the performance evaluation of a network intrusion detection system. Asian Journal on Quality, 11(1), 28-38.

[3]. Gillon, K., Branz, L., Culnan, M., Dhillon, G., Hodgkinson, R., & MacWillson, A. (2011). Information Security and Privacy-Rethinking Governance Models. Communications of the Association for Information Systems, 28561-570.

[4]. Thomas, M., & Dhillon, G. (2012). Interpreting deep structures of information systems security. Computer Journal, 55(10), 1148-1156.

[5]. Lin, P., Allhoff, F., & Rowe, N. (2012). Computing ethics war 2.0: Cyberweapons and ethics.Communications of the ACM, 55(3), 24-26.

[6]. Abraham, S.(2011). Information security behavior: Factors and research directions. Proceedings of the American Conference on Information Systems, Detroit. 462.

[7]. Patel, P., Langin, C., Yu, F., & Rahimi, S. (2012). Network intrusion detection types and computation. International Journal of Computer Science and Information Security, 10(1), 14-21.
[8]. Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25(2), 357-370. doi:http://dx.doi.org/10.1007/s10845-012-0683-0
[9]. Guozhu, M., Yang, L., Jie, Z., Pokluda, A., & Boutaba, R. (2015). Collaborative Security: A
[10].Alazab, M., Venkatraman, S., Watters, P. & Alazab, M. (2011). Zero-day malware detection based on supervised learning algorithms of API call signatures. Australasian Data Mining Conference (AusDM 11), Ballarat, 171-182.
[11]. Stegmaier, G.,& Bartnick, W. (2013). Another round in the chamber: FTC data securityrequirements and the fair notice doctrine. Journal of Internet Law, 17(5), 1-35.
[12].Alazab, M., Ventatraman, S., Watters, P., Alazab, M. & Alazab, A. (2011). Cybercrime: The case of obfuscated malware, in 7th International Conference on Global Security, Safety & Sustainability, Thessaloniki. doi: 10.1007/978-3-642-33448-1_28
[13].Baayer, J., Regragui, B., & Baayer, A. (2014). False positive responses optimization for intrusion detection system. Journal of Information Security, 5(2), 19-36.
[14].Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21,101.
[15].Barrios, R. (2013). A multi-leveled approach to intrusion detection and the insider threat. Journal of Information Security, 4(1), 54-65.
[16].Frenkel, K. A. (2017). Digital Transformation, Innovation and Security. CIO Insight, 1.
[17].Benferhat, S., Boudjelida, A., Tabia, K., & Drias, H. (2013). An intrusion detection and alert correlation approach based on revising probabilistic classifiers using expert knowledge. Applied Intelligence, 38(4), 520-540.
[18].Threat Stats. (2017). SC Magazine: For IT Security Professionals (15476693), 28(2), 6-7.
[19].Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to information technology crimes (Theft, Sabotage, Fraud).
[20]. Chen, H. M., Kazman, R., Monarch, I., & Wang, P. (2017). Can Cybersecurity Be Proactive? A Big Data Approach and Challenges. In Proceedings of the 50th Hawaii International Conference on System Sciences.
[21]. Chen, S., & Janeja, V. (2014). Human perspective to anomaly detection for cybersecurity. Journal of Intelligent Information Systems, 42(1), 133-153.
[22].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.
[23].Chivers, H., Clark, J., Nobles, P., Shaikh, S., & Chen, H. (2013). Knowing who to watch: Identifying attackers whose actions are hidden within false alarms and background noise. Information Systems Frontiers, 15(1), 17-34.
[24]. Clark, J., Beebe, N., Williams, K., & Shepherd, L. (2009). Security and Privacy Governance: Criteria for Systems Design. Journal of Information Privacy & Security, 5(4), 3-30.
[25].Comey, J. (2014). Federal Bureau of Investigation Director. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Retrieved from http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course
[26].Conger, S. (2009). Personal information privacy: A multi-party endeavor. Journal of Electronic Commerce in Organizations, 7(1), 71-82.
[27]. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. computers & security, 32, 90-101.
[28]. Cybenko, G. (2014). TIM Lecture Series – Cybersecurity Metrics and Simulation. Technology Innovation Management Review, 4(10), 43-45.
[29].D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643-658.
[30].D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. Journal of Business Ethics, 89(1), 59-71.
[31].Davis, A. (2012). Hacktivism. ITnow, 54(2), 30-31.

[32].Denning, P., & Denning, D. (2010). The profession of IT discussing cyber-attack.Communication of the ACM, 53(9), 29-31.
[33].Drtil, J. (2013). Impact of information security incidents: Theory and reality. Journal of Systems Integration, 4(1), 44-52.
[34].Elfeshawy, N., & Faragallah, O. (2013). Divided two-part adaptive intrusion detection system. Wireless Networks, 19(3), 301-321.
[35].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.
[36].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.
[37].Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. Informations System Frontiers, 15(1). doi:10.1007/s10796-010-9265-x
[38].Filshtinskiy, S. (2013). Cyber-crime, cyber-weapons, cyber-wars: Is there too much of it in the air? Communications of the ACM, 56(6), 28-30.
[39].Fishbein, M., & Ajzen, I. (2010). Predicting and Changing Behavior: The Reasoned Action Approach. Psychology Press, New York, NY.
[40]. Gasser et al., Don't Panic: Making Progress on the 'Going Dark' Debate, Berkman Center Research Publication. Retrieved from https://cyber.harvard.edu/pubrelease/dont-panic/
[41].Greengard, S. (2010). The new face of war. Communications of the ACM, 53(12), 20-22.
[42].Gritzalis, D., & Tejay, G. (2013). Cybercrime in the Digital Economy – Editorial. http://dx.doi.org/10.1016/j.cose.2013.08.002
[43].Hsu, J., & Shih, S. (2015). When does One Weight Threats more? An Integration of Regulatory Focus Theory and Protection Motivation Theory. WISP 2015 Proceedings.Paper 12.
[44].Hua, J., & Bapna, S. (2013). Who can we trust? The economic impact of insider threats.Journal of Global Information Technology Management, 16(4), 47-67.
[45].Hunker, J., & Probst, C. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. JoWUA, 2(1), 4-27.
[46].Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. Information Systems Frontiers, 15(1), 1-4. doi:http://dx.doi.org/10.1007/s10796-013-9419-8
[47].Ifinedo, P. (2011). An exploratory study of the relationships between selected contextual factors and information security concerns in global financial services institutions. Journal of Information Security and Privacy, 7(1), 25-49.
[48].Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.
[49].Jaiswal, A., & Jain, S. (2010). Database intrusion prevention cum detection system with appropriate response, International Journal of Information Technology, 2(2), 651-656.
[50].Kim, S., Wang, Q., & Ullrich, J. (2012). A Comparative Study of Cyberattacks. Communications of the ACM, 55(3), 66-73. doi:10.1145/2093548.2093568
[51].Kyong-jin, K., Seng-phil, H., & Joon Young, K. (2013). A Study of Privacy Protection from Risk of Hijacking Data. International Journal of Multimedia & Ubiquitous Engineering, 8(1), 235-244.
[52].Lai, F., Li, D., & Hsieh, C.T. (2012). Fighting identity theft: The coping perspective. Decision Support Systems, 52(2), 353-363.
[53].Lane, G., & Sui, D. (2010). Geographies of identity theft in the US: understanding spatial and demographic patterns, 2002–2006. GeoJournal, 75(1), 43-55.
[54].Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M.,H. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review, 37(12). 1049.
[55].Lobel, H. (2012). Cyber-war INC.: The laws of war implications of the private sector's role in cyber conflict. Texas International Law Journal, 47(3), 617-640.
[56].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.
[57]. Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers & Security, 31(5), 673-680.

[58].Panigrahi, S., Sural, S., & Majumdar, A. (2013). Two-stage database intrusion detection by combining multiple evidence and belief update. Information Systems Frontiers, 15(1), 35-53.
[59]. Patel, A.,Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. Information Management & Computer Security, 18(4), 277-290. http://dx.doi.org/10.1108/09685221011079199
[60].Pérez, M.,Mármol, F., Pérez, G., & Gómez, A. (2013). RepCIDN: A reputation-based collaborative intrusion detection network to lessen the impact of malicious alarms. Journal of Network and Systems Management, 21(1), 128-167.
[61].Posey, C.,Roberts, T., & Lowry, P. (2011). Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. The Dewald Roode Information Security Workshop. Blacksburg, VA, USA. IFIP WG 8.11/11.13.
[62].Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How Effective Is Your Security Awareness Program? An Evaluation Methodology. Information Security Journal: A Global Perspective, 21(6), 328-345. doi:10.1080/19393555.2012.747234
[63].Schuesster, J. H. (2013). Contemporary threats and countermeasures. Journal of InformationPrivacy & Security, 9(2), 3-20.
[64].Schwartz, M. J. (2012). 10 steps to protect against insider threats. InformationWeek, (1328), 12.
[65].Shameli-Sendi, A., Ezzati-Jivan, N., Jabbarifar, M. & Dagenais, M. (2012). Intrusion response systems: survey and taxonomy, International Journal of Computer Science Network Security, 12(1), 1-14.
[66].Siponen, M, Pahnila, S., & Mahmood, M. (2010). Compliance with information security policies: An empirical investigation. http://doi.ieeecomputersociety.org/10.1109/MC.2010.35
[67]. Siponen, M, Pahnila, S., & Mahmood, M. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224.
[68]. Sommestad, T.,& Hunstad, A. (2013). Intrusion detection and the role of the system administrator. Information Management & Computer Security, 21(1), 30-40. http://dx.doi.org/10.1108/09685221311314400
[69]. 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.
[70].Stamos, A.,(2016). Addressing Security Blindspots through Culture. Retrieved from https://www.facebook.com/notes/alex-stamos/addressing-security-blindspots-through-culture/10154390896047929
[71].Stanciu, N. (2013). Technologies, methodologies and challenges in network intrusion detection and prevention systems. Informatica Economica, 17(1), 144-156.
[72].Stephenson, P. (2012). Endpoint security. SC Magazine, 23(8), 32. Retrieved fromhttps://www.scmagazine.com/eset-endpoint-security/review/6640/
[73].Tarafdar, M., D'Arcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. MIT Sloan Management Review, 56(2), 61-70.
[74].Taylor, R.,& Robinson, S. (2014).The roles of positive and negative exemplars in information security strategy. Academy of Information and Management Sciences Journal, 17(2), 57-79.
[75].Vance, A.,Lowry, P. B., & Eggett, D. (2013). Using Accountability to Reduce Access Policy Violations in Information Systems. Journal of Management Information Systems, 29(4), 263-290. doi:10.2753/MIS0742-1222290410
[76].Vance, A.,Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management, 49(3), 190-198.
[77].Willison R.,& Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly, 37(1).
[78].Yaseen, Q., & Panda, B. (2012). Insider threat mitigation: Preventing unauthorized knowledge acquisition. International Journal of Information Security, 11(4), 269-280. doi:http://dx.doi.org/10.1007/s10207-012-0165-6
[79].Yazdani, N., & Murad, H. S. (2015). Toward an ethical theory of organizing. Journal of Business Ethics, 127(2), 399-417. doi:http://dx.doi.org.library.capella.edu/10.1007/s10551- 014-2049-3
[80].Young, S. (2013). Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches. Journal of Corporation Law, 38(3), 659-679.
[81].Zhou, C., Leckie, C., & Karunasekera, S. (2010). A survey of coordinated attacks and collaborative intrusion detection. Computers & Security, 29(1), 124-140.

AUTHORS' BIO

Alain Loukaka: Alain Loukaka is a Ph.D. candidate in the Information Security and Information Assurance program at the Capella University, Minneapolis, USA. Alain study is an exploratory research on cybersecurity exploits and an advanced method of detection beyond current know application. 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 plan 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 Majmaah University, Majmaah, KSA. Dr. Rahman's research interests includeInformation Assurance and Security, Digital Forensics, Software Engineering education, Software Testing & QA, Cloud Computing, Mobile Application Development, and Web Accessibility. He has published over 100 peer-reviewed articles and is a member of many professional organizations including IEEE, ACM, ASEE, ASQ, ISACA, ISCA, and UPE.