THE EFFECT OF INFORMATION TECHNOLOGY USING ENTERPRISE SECURITY RISK MANAGEMENT

Michael O. Adekanye[1] and Shawon S. M. Rahman, Ph.D.[2]

[1]Address: P.O Box 9201, Trenton NJ 08650, USA
[2]Associate Professor, Dept. of Computer Science & Engineering, University of Hawaii-Hilo, 200 W. Kawili Street, Hilo, HI 96720, USA,

ABSTRACT

The philosophy of Enterprise Security Risk Management (ESRM) drives a risk-based approach to managing any security risks, physical or logical and holistically applies to every security process. There are globally established risk principles that are common among any developed risk management standard. This model associates the relationship of risk principles to the practice of managing security risks. The ESRM processes, when successfully and consistently adapted to a security program, will define what a progressive security program looks like, drive strategic through initiatives, build the business understanding of security's role to develop a budgeting strategy, and initiate board-level, risk-based reporting. The management security leader's role in ESRM is to manage risks and unthinkable harm to enterprise assets and stockholder in partnership with the business leaders whose assets are exposed to those risks management. ESRM is part of educating business leaders on the realistic of impacts. These identified risks, presenting any potential strategies to mitigate those impacts, and enacting the option chosen by the business in line with acceptable levels of business risk tolerance. The present data should be used to showcase how our service helps identify, evaluate, and mitigate risks at face value that would be detrimental to a company's long-term prosperity. We need to show how using our security risk management will ultimately benefit the company's work by improving policies and procedures and reducing other expenses through the use of risk principles management.

KEYWORDS

Enterprises Security Risk Management, ESRM, Maturation of a Profession, Unfettered Rules, Risk Mitigation, Risk Mechanism, Enterprise Risk Management, Risk Principles Management, Manage Security Programs,

1. INTRODUCTION

The Enterprise Security Risk Management (ESRM) is a new philosophy and methodology for managing security programs through the use of traditional risk principles. As a philosophy and life cycle, ESRM is focused on creating a business partnership between security practitioners and business leaders to more effectively to protect against security risks. The acceptable business tolerances as defined by business owners and stakeholders. This paper explores the basics gap between the ESRM philosophy and life cycle and also shows how embracing the ESRM philosophy and implementation works.

As a security professional, have we noticed that our other company do not always define security in the same way? Perhaps security interests and business interests have become misaligned. Based on the new approach from the author Arena[2]. The ESRM has the potential to transform the practice of any security completely. ESRM is based on an extended method of managing an effective security program through the use of risk principles management by companies around the world. The present principle of ESRM principles can change the way we perform our jobs, the

way we see our roles and the way others see them from another perspective. The ways we protect our enterprises, our assets, and our employees. And ESRM helps us in our careers, by increasing our personal and professional satisfaction and by ensuring that security is seen as it deserves to be as a professional discipline. ESRM can help the organization and our security program to be successful[3]. Whether the threats are informational, cyber, physical security, asset management, or business continuity, all were included in the holistic, all-encompassing ESRM approach which will move our task-based to risk-based security.

As professional security, we may already practice some of the components of ESRM. Many of the concepts such as risk identification, risk transfer and acceptance, crisis management, and incident response will be well known to us[3]. Many organizations with a comprehensive, holistic way that ESRM represents and even fewer that communicate these principles effectively to key decision-makers. ESRM offers very skills and straightforward, realistic, and actionable approach dealing effectively with all the distinct types of security risks facing individual as a security practitioner in the organization[15]. The ESRM is implemented in a life cycle of risk management including the Asset assessment and prioritization, risk assessment and prioritization, Risk treatment mitigation and continuous improvement. Throughout the ESRM[7] concepts and applications, the authors release the tools give the company the materials that will help an employee to advance individual in the security field, no matter what the situation; if we are a student, a newcomer, or a seasoned professional.

The realistic case studies with questions to help an individual to assess security program, through-provoking discussion and questions, useful figures and tables as references for the article[7] Redefining how security enterprises work, everyone thinks about the role of security in the enterprise security risk area; the security organization can focus on working in partnership with business leaders and CIO, including the stakeholders to identify and mitigate the use of security risk. As we begin to use ESRM incorporation; we will experience greater personal and professional satisfaction as a security professional, and we will become a recognized and trusted partner in the business critical effort of protecting our enterprise and all its assets.

2. THE MATURATION OF A PROFESSION

As the supporter of ESRM grew in number and further create a more significant career, implementing the ideas in our various organizations, the core idea of ESRM continued to grow and mature. Security practitioners started teaching ESRM educational sessions, as well as writing white papers, articles, and case studies. They spoke about the driving philosophy of ESRM, and most importantly, communicated the success stories of implementation and ongoing management of many companies bringing more converts into the fold [3]. The collective lessons learned from ESRM adopters, in turn, drove many of us to realign and optimize our departments and individual functions to be more consultative and tightly tied to our respective business's strategy, providing more and more real-world success metrics for the ESRM.

2.1. PURSUE CONTINUOUS IMPROVEMENT

Enterprise security risk management effort starts as a discrete project but requires ongoing consideration [9]. Those charged with security must keep current with threats and trends within the organization and beyond. Security incidents [18][22]need the proper cause of analysis this should include team members beyond those directly charged with security. Incidents represent apparent opportunities to reassess risks and responses, and threat analysis and response plans should regularly be reviewed, regardless of whether an event has ESRM Principles and policies in Place.

Figure 1: Pursue Continuous Improvement occurred

2.2. UNFETTEREDRULES,BRING YOUR OWN DEVICE(BYOD)

BYOD can be a cost-effective way to allow users to use tools they're more comfortable and familiar with [4] policies and technical controls to manage those are critical. Left unchecked, they can result in the loss of sensitive data, such as source code or client information. Many corporations think there were immune to hacking or device destruction by a virus, so they forget to close the back door, leaving backup devices unsecured on filing cabinets or in cubicles, and the lack of screensaver passwords to secure laptops and desktops when unattended. Assuming that endpoint security and passive scans suffice[4]. The prevalence of web applications makes almost every site vulnerable to cross-site request forgeries, XSS cross-site scripting[18], and more. Strong sites required require robust security such as the Open Web Application Security Project (OWASP) technology[17]. OWASP is a unique software company that positions herself to provide impartial, information about AppSec to individuals, and corporations, universities, government agencies and departments' organizations around the world. The company Operated in a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security[24] [25]. Networks must be proactive, continually monitoring for threats and understanding new risks.

2.3. THE NECESSARY SKILL SETS

The ESRM leader used a wide range of skill sets to be to be successful. According to the author[1], these skills are less related to security knowledge than they are in the business world. Leading the enterprise's security risk management effort is about being supportive to the business objectives and the board's goals, and aligning the company with those and pushing the program as part of the board's overall business aims and objectives[1]. To understand the pure and innovative business, we do not have to be a Chief Financial Officer (CFO) or developer or retailer; what we have to be is a very good generalist and a good leader, somebody who can make decisions and get people on highly innovative on different functions in the organizations to engaged in trust[5]. What we are able to provide is the change in management innovation and the use of an appropriate approach to solve problems.

The implementation of a program involves change, and if we have got a skill set that includes an understanding of business processes and understanding the business, as we would if we were a consultant coming in to examine process flows and working relationships, that skill set helps with a risk management program[5] [23]. Just as significant know who to go to for help; we have people in finance we can call on for that skill set. We have worked closely with IT and IT

development, so if we have any knowledge gap regarding skill sets with IT infrastructure and technical details. We have got people within the organization that we work with; whom we can call on[14]. What's most important is a broader understanding of what is driving and therefore what can influence the business beyond security and malicious threat [27]concerns that we have every day.

2.4. COMMUNICATION SKILLS

It's really about personal ability to communicate, understand how others interact. We are not sure that's it is something that it has to be learned, but we think an individual can develop it. The first skill is to be able to get past the initial mistrust. It's fostering those relationships and letting those people know it's not us coming in and taking our headcount, but the ability to articulate that this process is for the betterment of the organization[2] [16]. It is not about building our Corporation or convergence in the sense that we're going to put two, three departments together it's the ability to communicate through and come up with that soft approach and ability to talk business in the right sense. The skills that help the CSO and CIO communicate the skills throughout the organization.

2.5. THE BENEFIT OF TECHNOLOGIES ON INFORMATION SECURITY

The technological progress brings clear benefits for the companies and the development of the profession[12], helping to reduce the costs by increasing the productivity level and enhancing process automation. However, we must be aware that each of these new technologies has a common challenge, the security of sensitive data. In the paper, we analyze the data security from the perspective of these existing and emerging technologies that influence the accounting field, along with the exposure of the possible impact of security incidents[13]. The international accounting bodies emphasize the necessity to develop the appropriate skills for protecting the data and assuring confidentiality, integrity, and availability of the information by using efficient controls[1]. By adopting these technologies in the accounting field, the risk of sensitive data exposure increases and this regard the practitioners need to understand the necessity of preventing security incidents, even more, now as the most significant amount of vulnerable data is produced by the accounting and financial departments[26].

2.6. FRAMEWORK APPROACH IMPROVEMENT

The organization's ability to manage risk effectively is to depend on its intentions and its capacity to achieve those intentions to the highest[7]. The purpose and role are referred to as its risk management framework and is part of its system of governance and management. The quality of the structure is important because effective risk management that requires:

a) clear expectations from the top;
b) appropriate capability skills, resources, support
c) sound relationships with
d) stakeholders
e) integration is known of necessary risk management practices into the day to day activities and accountabilities of the management team
f) a firm commitment to continually learn and improve the risk management framework should not attempt to replace the natural capability of people to manage risk; instead, it should enhance an actual good practice among those who have reliable and comprehensive ideas consistent in dealing with issues

For this to occur and for the required capability to be achieved, the organization requires, such as

a) A set of suitable tools
b) A smart and coherent approach to training and communication process tools competently and consistently and
c) A model approach that signals and reinforces the correct behavior and way of thinking.

The typical elements of a framework and an illustration of how this supports the integration and skill of the risk management process are shown in the table below.

2.7. THE IMPACT OF EDUCATING BUSINESS LEADERS ON SECURITY STRATEGY

The ESRM is a management process used to effectively manage security risks, both proactively and reactively, across an enterprise setting. ESRM [2] continuously assesses the full scope of security-related risks to an organization and within the enterprise's complete portfolio of assets. The management process quantifies threats, establishes mitigation plans, identifies risk acceptance practices, manages incidents, and guides risk owners in developing remediation efforts. ESRM involves in educating business leaders on the realistic impacts of identified risks, presenting potential strategies to mitigate those impacts, and then enacting the option chosen by the business in line with acceptable levels of risk business with tolerance[12]. To bring the discussion into the appropriate context, we want to explain my journey through the security profession and share why we have been so focused on moving away from the old break glass when needed approach that so often characterizes my interactions with the non-security functions in my organization, and towards the ESRM approach.

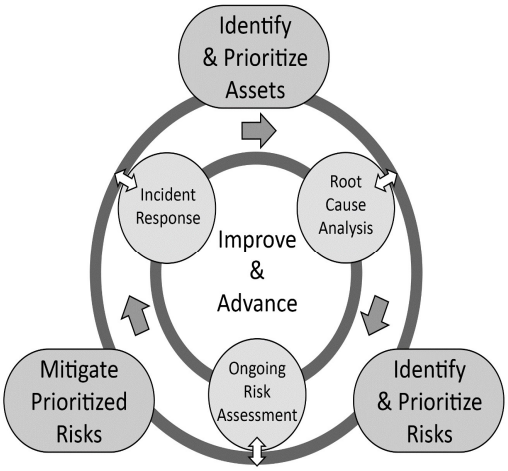

Figure 2 - The ESRM Life Cycle

The ESRM is a security program management tool with detail links and activities to an enterprise direct mission and goals through management methods. Leader's role in ESRM is to manage security risks in the enterprise assets area. Those business leaders whose assets were exposed to the risks ought to have skills training in place to make a full impact to identified risks. The potential strategies to mitigate those impacts, and then enacting the option chosen by the business in line with acceptable levels of risk business with tolerance. To bring the discussion into the appropriate context, we want to explain our journey through the security profession and share our thought on why we have been so focused on moving away. New thinking is needed to break away from an old approach that. Somehow characterizes as often interactions with the non-security

functions in my organization and towards the ESRM approach. This approach is detailed in the ESRM Life Cycle Model

The ESRM becomes an Australian Secret Intelligence Service (ASIS) strategic priority[14]. Today, every part of the business world is digitized and networked. A few years ago, an organization may have supported a single network of desktops within the confines of a physical office. No longer the case nowadays; data is accessed and manipulated from everywhere, not just through workstations and desktop. Computers in an office, with laptops at home, or even on cell phones and in airports, cafes, and other public places.E-commerce customers also submit credit card numbers via web forms without a second thought[7]. As the flexibility and robustness of digital devices continue to grow, security threats[19][20]are also becoming more sophisticated. Hackers deploy bots to enact DDoS (Distributed Denial of Service) attacks, and cause mayhem through pretesting, where they send an email under the guise of an authority figure or business to infect vulnerable systems with Trojans, viruses, or other malware.

Additionally[1], the prevalence of Internet of Things (IoT) devices opens pathways to database disaster. Therefore, a new approach to security is necessary. Enterprise security management looks at policies and infrastructure from a holistic perspective and holds that all parts of an organization contribute to safety[8]. With this approach, new enterprise tools, such as SIEM security information and event management platforms, automate the monitoring and management of threats, software updates, reporting for compliance, and more. In this article, we have discussed enterprise security management and its derivatives, and explain common setbacks and difficulties in protecting our enterprise from security breaches[20]. Then, we have explored the best practices and how software tools can improve our security systems, and offer a heuristic for choosing the right solution for our organization.

3. HOW TO IMPLEMENT ENTERPRISE SECURITY RISK MANAGEMENT

If enterprise security management provides the organizational structure and culture for enacting security plans, enterprise security risks management[19] is the process of identifying risks and eliminates the threats, determining how to mitigate them, and documenting policies and best practices to proactively and reactively address future occurrences[3]. The approach ESRM considers a project with its vision, mission, and goals. The concept is to protect the assets of an entire organization so that it can execute its larger business vision and mission. The purpose of continually identifies analyses, and responds to risks to the business. The goals create, maintain, and promote policies and best practices to protect the organization against security risks.

To understand what's at risk, one must know what assets and critical infrastructure and resources on have, and why they are essential[9]. Threat Modeling and Assessment and Risk Assessment very important. These were the reasonable and current security of the enterprise security risk management. Also, what do we consider our vulnerabilities and what are the risks to each asset? Who else might want to impede our business? Some significant dangers include the requirement for SSL and authorization checks and measures against SQL injection.

3.1 RISK MITIGATION ACTION POINTS

Coordinate with the stakeholders to determine how to manage risks and identify security objectives. Options include stopping risky activities, planning mitigation for security events, or only accepting the risk. Creating a corporate security policy is essential, and must cover all aspects and assets of the organization. The enterprise security risk management (ESRM) is a progressive practice which, when combined with security convergence, these can help organizations such as my corporation to set up comprehensive SCRM processes. Aspects of

enterprise security risk management can include Supply chain risk management; Physical asset protection; Human resource security; Information security[26]; Communications security and Continuity management. The Organizational behaviors that limit security; Not long ago, we experience computers with a powered-down modem, and an office with a locked front door would sufficiently protect our network and data information. But as the innovation progress, we no longer have access to the model. Instead, today's security must be strategic, systematic, and repeatable. They followed ways and many organization sabotage their security; by inviting problem on their system.

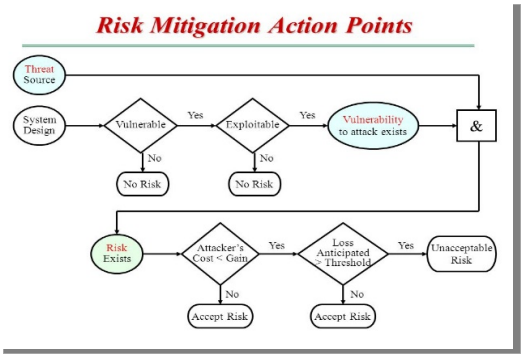

Figure 3: Risk Mitigation Action Points

3.2. THE FRAMEWORK FOR RISK MANAGEMENT

After many years of strategic, tactical, practical experience in evaluating and enhancing structures for risk management in organizations[9], Broadleaf believes that immediate success depends as much on the manner in which any changes to a structure are developed and implemented as it does in the detail of the tools and written materials generated[9]. We strongly recommend to our clients that we helped through the management of change process, where key internal stakeholders are carefully involved and engaged in evaluating the existing approach and in planning how, where and when enhancements will be made. The core of this management of the change process involves internal stakeholder representatives participating in facilitated gap analysis and evaluation that leads to a bright and practical enhancement and implementation plan. To enable those stakeholder representatives to compete effectively, they need to be well informed on current risk management thinking and shown examples drawn from other organizations of elements of a risk management framework[3]. The approach has the added benefit that the participants of this process then become the organization's Champions who were motivated to lead the implementation process in their departments and functions. They acted to convince their superiors of the merits of the approach and stimulate acceptance and use[6]. To be successful and efficient, management to change attitude requires:

a) An accepted accurate representation of the current arrangements for managing differences between the forms of risks at present situation.
b) Fundamental concepts of risk management at the desired goals regarding risk management and the framework process for the clearly understood by those sponsoring the change.
c) A bright idea and accepted appreciation of the elements of the existing structure that need to be enhanced or improved and the nature of those changes and any additional features that need to be created what needs to change
d) Exploration of options, constraints, enablers and critical paths leading to an appropriate plan of actions with timings

e) A clear commitment to the program and its implementation through the allocation of suitable resources by senior management and by their continued oversight of progress[13].

Steps can be taken to separate the results from the senior management. However, after many years and numerous attempts, we have found that most efficient approach, and the one that gains the highest degree of ownership and endorsement, is to involve representatives of senior internal stakeholders in all the steps over a short space of time.

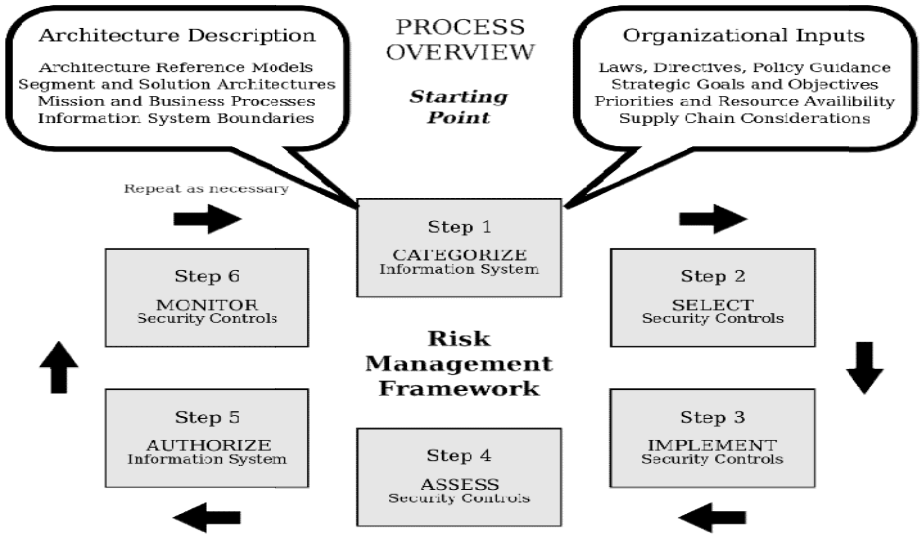

Figure 4: The framework for risk management

4. TECHNOLOGICAL INNOVATION DECISION MAKING

Even though the benefits of the emerging technologies presented above are considered universally accepted, it is essential to understand the local impact of these technologies, regarding the accounting profession[6]. Another study concerning the willingness of accountants in regards to allowing cloud solutions has emphasized that the business shows a high level of interest in the benefits brought by cloud computing and consider that migration as representing a positive aspect[1]. However, we must not overlook that the usage of new technologies requires the existence of prepared professionals that will be able to exploit these resources efficiently.

Based on the highlights the fact that the accounting profession has a significant role in the information technology and acceptance of emerging technologies, such as cloud accounting and information risk management[1]. The author considers that the accountants should act as an intermediary between the IT departments and the administration, by advising the suitable IT solutions that can add value to the organization, after performing appropriate analyses based on cost efficiency. The most significant benefits identified in this study are considered to be: a higher degree of innovation, rapidity and increased accuracy[7]. By analyzing the challenges presented, two critical drawbacks are addressed: the facts that most cloud providers do not offer a solution for local backup and the rigidity of cloud solution compared with desktop solutions.

Due to the dependency of IT enhancements that can facilitate the operational processes of organizations, the security aspects of information risk management seem to be the biggest drawback identified by the researchers in the Asia accounting profession. Accounting practitioners rely heavily on the security of data in transit and certifications of the cloud supplier. The IT professionals with the overall safety of the applications and the existence of a disaster recovery plan are considered to be a key differentiator[7] Moreover, shared data information risk management and multi-tenancy issues are deemed to be a significant drawback for the accounting professionals[10]. This outcome shows that there are differences in emerging information risk management expectations between the financial and IT departments when it comes to the selection of the cloud supplier, an aspect that can influence the overall security[27] of the solution, in the scenario in which the accounting department should mitigate any possible migration.

Mobile technologies are being adopted more quickly and efficiently compared with the other emerging technologies presented, a point that can be explained through the general preference of using Smartphones and tablets[4] Benefits such as continuous access, better connectivity, and reduced costs, when are used with cloud platforms[4] qualifies mobile technologies as a critical differentiator in the current local economic context. However, some of the most addressed drawbacks and challenges of this technology are limited resources, small screens, and connectivity issues. The general trend of adopting the BYOD (Bring Your Own Device) concept comes with a broad range of security issues that must be addressed, such as physical security of the device, software vulnerabilities,
and access control.

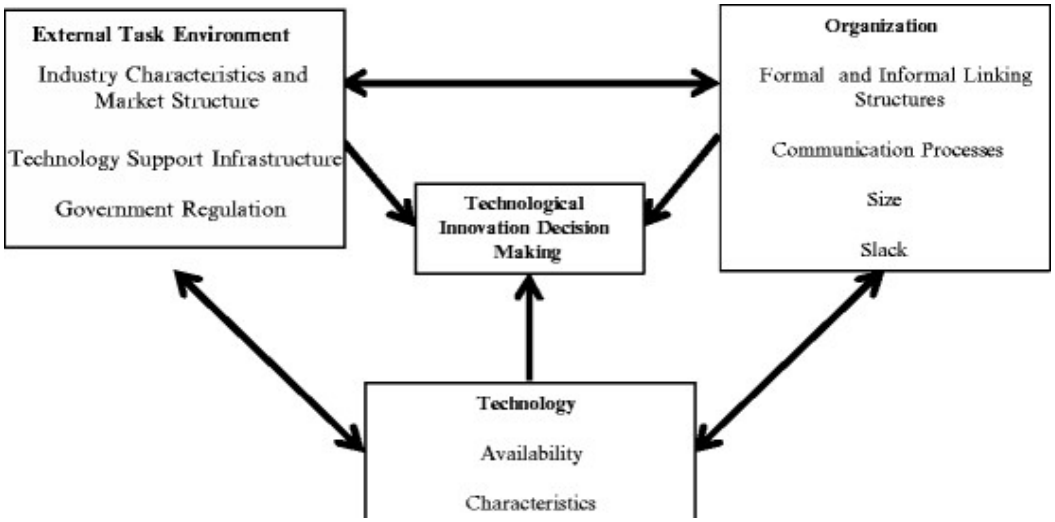

Figure 5: Technological Innovation Decision Making

5. CONCLUSION

The Enterprise's Security Risk Management (ESRM) is a security program management risk with a detailed approach that links activities to an enterprise's mission. The business goals through risk management methodology[15] [21]. The security leadership role in ESRM to manage risks from enterprise management partnership assets to business leadership. The ESRM which involves in educational business leadershipon the realistic of impacts. To identify risks with potential strategies to mitigate those impacts, and then enacting the option of chosen by the business in line with acceptable levels of risk and resilience with the goal. The most significant, perhaps with the

awareness of enterprises security risks management. In the world of enterprise risk management, the business owners are the owners of all risks.

Depending on the asset in question, the owner of that asset whether a data hall of information, a warehouse of human capital, or brand reputation in the organization which determines the treatment of any risk to that asset[2]. The security practitioner in an ESRM programme is required by his or her philosophy to ensure that business leaders understand the risks to their assets. The philosophy drives all parts of the business to recognize and proactively deal with threats in the management and security departments. This integration provides a stable platform for the continuous development of a holistically secure enterprise[11]. The analysis of the Risk Management Approach with the various architecture levels to demonstrate how organizations could gain from the integration of enterprise risk management. The core levels of the organization and focusare on their investments to ensure a clear mission of readiness. With correct cyber health by implementing countermeasures across IT's enterprises. To ensure mission continuity as well as develop future state architectures in delivering improved information security[10].

REFERENCES

[1] Al-Htaybat, K. & von Alberti-Alhtaybat, L. (2017) "Big Data and corporate reporting: impacts and paradoxes", Accounting, Auditing & Accountability Journal, vol. 30, no.4: 850-873

[2] Arena, M., Arnaboldi, M., &Azzone, G. (2011). Is enterprise risk management real?.Journal of Risk Research, 14(7), 779-797. doi:10.1080/13669877.2011.571775

[3] Baxter, R., Bedard, J. C., Hoitash, R., &Yezegel, A. (2013). Enterprise Risk Management Program Quality: Determinants, Value Relevance, and the Financial Crisis. Contemporary Accounting Research, 30(4), 1264-1295. doi:10.1111/j.1911-3846.2012.01194.x

[4] Bradley, J., Loucks, J., Macaulay, J., Medcalf, R. &Buckalew, L. (2012) „BYOD: A Global Perspective, Harnessing Employee-Led Innovation", available online at http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYODHorizons-Global.pdf (accessed March 15th 2017)

[5] Caldarelli, A., Ferri, L. &Maffei, M. (2017) "Cloud Computing Adoption in Italian SMEs: A Focus on Decision-making and Post-implementation Processes", Reshaping Accounting and Management Control Systems, 53-76

[6] Frigo, M. L., &Ubelhart, M. C. (2016). Human capital management: The central element of all risk. People and Strategy, 39(1), 42–46.

[7] Gupta, S., & Saini, A. K. (2013). Information System Security and Risk Management: Issues and Impact on Organizations. Global Journal Of Enterprise Information System, 5(1), 31-35.

[8] Huth, C. (2013). The insider threat and employee privacy: An overview of recent case law. Computer Law & Security Report, 29(4), 368–381. Retrieved from http://www.sciencedirect.com/science/article/pii/S0267364913001052?np=y

[9] Hwankuk, K., Kyungho, L., &Jongin, L. (2017). A Study on the Impact Analysis of Security Flaws between Security Controls: An Empirical Analysis of K-ISMS using Case-Control Study. KSII Transactions On Internet & Information Systems, 11(9), 4588-4608. doi:10.3837/tiis.2017.09.022

[10] National Institute of Standards and Technology. (2010). Guide for Applying the Risk Management Framework to Federal Information Systems. Special Publication 800-37, Rev 1. (Gaithersburg, MD: National Institute of Standards and Technology.)

[11] National Institute of Standards and Technology (NIST). (n.d.). Risk management framework overview. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/framework.html

[12] Petruzzi, J., &Loyear, R. (2016). Improving organisational resilience through enterprise security risk management. Journal Of Business Continuity & Emergency Planning, 10(1), 44-56.

[13] Ray, Bonnie K; Tao, Shu; Olkhovets, Anatoli; Subramanian, Dharmashankar. EURO Journal on Decision Processes; Heidelberg Vol. 1, Iss. 3-4,(Nov 2013): 187-203. DOI:10.1007/s40070-013-0013-6 npKey=5e7ab5151c75b3dbb6d5aa532fa90456ded4a947dcb7c3d74459ee872656c319

[14] Rimböck, A., &Loipersberger, A. (2013). Integral risk management: steps on the way from theory to practice. Natural Hazards, 67(3), 1075–1082.

[15] Yaraghi, N., & Langhe, R. G. (2011). Critical success factors for risk management systems. Journal Of Risk Research, 14(5), 551-581. doi:10.1080/13669877.2010.547253

[16] Loukaka, Alain and Rahman, Shawon; “Discovering New Cyber Protection Approaches From a Security Professional Prospective”; International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.4, July 2017
[17] Al-Mamun, Abdullah, Rahman, Shawon and et al;“ Security Analysis of AES and Enhancing its Security by Modifying S-Box with an Additional Byte ”; International Journal of Computer Networks & Communications (IJCNC), Vol.9, No.2, March 2017
[18] Opala, Omondi John; Rahman, Shawon; and Alelaiwi, Abdulhameed; “The Influence of Information Security on the Adoption of Cloud computing: An Exploratory Analysis”, International Journal of Computer Networks & Communications (IJCNC), Vol.7, No.4, July 2015
[19] Rader, A., Marc and Rahman, Syed (Shawon); “Exploring Historical and Emerging Phishing Techniques and Mitigating the Associated Security Risks”; International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.4, July 2013
[20] Opala, John, Omondi and Rahman, Syed (Shawon);“Corporate Role in Protecting Consumers from the Risk of Identify theft ”; International Journal of Computer Networks & Communications (IJCNC), Vol.5, No.5, September 2013
[21] Neal, David and Rahman, Syed (Shawon); “Video Surveillance in the Cloud?”; The International Journal of Cryptography and Information Security (IJCIS), Vol.2, No.3, September 2012
[22] Halton, Michael and Rahman, Syed (Shawon); "The Top 10 Best Cloud-Security Practices in Next-Generation Networking"; International Journal of Communication Networks and Distributed Systems (IJCNDS), Vol. 8, Nos. ½, 2012, Pages:70-84
[23] Schuett, Maria and Rahman, Syed (Shawon); “Information Security Synthesis in Online Universities”; International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011
[24] Slaughter, Jason and Rahman, Syed (Shawon); " Information Security Plan for Flight Simulator Applications"; International Journal of Computer Science & Information Technology (IJCSIT), Vol. 3, No 3, June 2011
[25] Bisong, Anthony and Rahman, Syed (Shawon); "An Overview of the Security Concerns in Enterprise Cloud Computing "; International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011
[26] Hossain, Md; Hossain, Nazmul; Shahid, Afridi and Rahman, Shawon; “Security Solution of RFID Card Through Cryptography”; The Third International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys 2017), Guangzhou, China, December 12-15, 2017
[27] Okonofua, Henry and Rahman, Shawon; “Evaluating the Risk Management Plan and Addressing Factors for Successes in Government Agencies”; 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18), August 1-3, 2018, New York, USA

AUTHORS’ SHORT BIO

Michael Adekanye is a Ph.D. student at the Capella University in Information TechnologySpecialization: Info Assurance and Security Program.His research interests include the effectof Cybersecurity on Infrastructures vulnerabilities threat against systems collusion and how to mitigation robust password authentication on all systems.

Dr. Shawon S. M. Rahman is an Associate Professor of Computer Science at the University of Hawaii-Hilo and a part-time faculty of Information Technology, Information Assurance and Security Program at the Capella University. Dr. Rahman’s research interests include software engineering education, information assurance and security, digital forensics, web accessibility, cloud-computing, and software testing and quality assurance. He has published over 110 peer-reviewed articles in various international journals, conferences, and books. He is an active member of many professional organizations including IEEE, ACM, ASEE, ASQ, and UPE.