Enhancing Network Security Environment by Empowering Modeling and Simulation Strategy

(Cyber Protect Simulation Lesson Learned)

Rudy Agus Gemilang Gultom
Deputy for Strategic Studies
The National Resilience Institute of the Republic of Indonesia (Lemhannas RI)
Jakarta, Indonesia
e-mail: rudygultom@lemhannas.go.id

Baskoro Alrianto
Bureau of Telematics
The National Resilience Institute of the Republic of Indonesia (Lemhannas RI)
Jakarta, Indonesia
e-mail: karotelematika@lemhannas.go.id

***Abstract*—This paper provides an overview based on cyber protect simulation experiences to enhance network security environment by empowering modeling and simulation strategy. Cyber protect is a simulation tool developed by the US Defense Information Systems Agency (DISA). Cyber protect simulation is an integral part of cyber security for information leaders course at National Defense University (NDU), Washington, DC. USA. Strategic thoughts can be implemented during cyber protect simulation exercises. Brilliant ideas in simulating an organization network security environment become good lesson learned. The implementation for proper defense strategy could secure an organization Local Area Network (LAN) from various threats, attacks and vulnerabilities in concrete and abstract levels. Countermeasure strategy, which is implemented in this simulation exercise is presented as well. At the end of this paper, an initial network security framework concept, so called The Six-ware Framework concept (The SWF concept) has been introduced.**

Keywords-cyber protect simulation; threats, attacks and vulnerabilities; countermeasures strategy; network security framework and models

I. INTRODUCTION

Nowadays, as the cost of information processing and internet accessibility falls, civilian, military and government organizations security environments are becoming increasingly vulnerable from cyber threats or attacks, e.g., network intrusions, DoS/DDoS, phishing, spoofing, viruses, flooding, etc. At this point, the information security manager might allocate budget, spreading it for network defense tools, e.g., anti-virus software, firewalls, intelligent routers or expensive modeling and simulation (M&S) tools. M&S is an effective technique to support better understanding for information security managers in concrete and abstract levels [1]. M&S can be used to identify weaknesses proactively and it can also provide education and training using "what if" scenarios reactively. Ultimately when new threats appear the ability of an organization to respond is significantly enhanced.

One good lesson learned in the context of information security issue today is the phenomenon of Panama papers where over 11.5 million files have been leaked including 2.6 terabytes of data. E-mails accounted for the majority of exposed records (4,804,618 files), followed by database formats (3,047,306), PDFs (2,154,264), images (1,117,026), text documents (320,166) and other (2,242) files (see Figure 1). At this point it is still unclear whether the 11.5 million files were obtained through hacking (data breach) or leaked from someone inside of the Panamanian law firm (insider leak). But from a cyber protect perspective, the lessons are nearly identical either way [2][3][4][5].

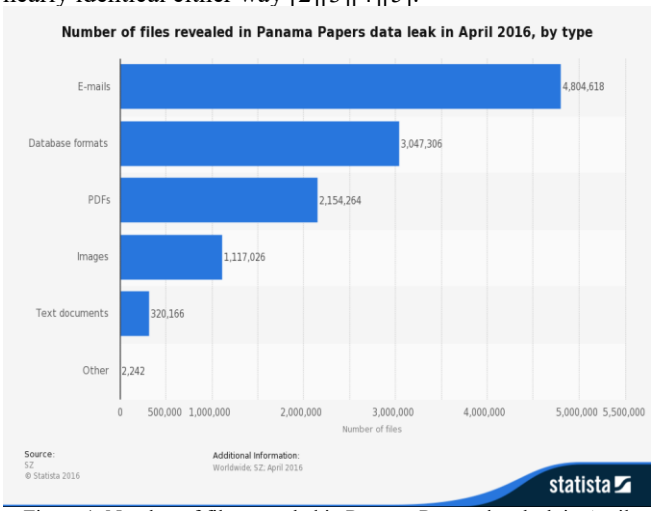

Figure 1. Number of files revealed in Panama Papers data leak in April 2016 by type [5]

The purpose of this paper is to enhance security awareness environment within an organization in order to overcome the various security threats, attacks and vulnerabilities through empowering modeling and simulation strategy based on network security framework models. It also meets the demands of the countermeasures strategy and policy of an organization.

The rest of the paper is structures as follows. Section II presents the cyber protect simulation tool. Section III presents security threats, attacks and vulnerabilities discussion. Section IV explains countermeasures strategy and policy. Section V discusses why an organization needs to adopt an appropriate network security framework model

 ISBN: 978-1-61208-475-6

to enhance its network security environment. Section VI describes contribution of this paper by proposing a new concept proposal, called The Six-Ware Framework (The SWF). This contribution is a very early concept inspired by cyber protect simulation experiences. Section VII contains concluding remarks and future work for the SWF concept development.

II. WHAT IS CYBER PROTECT?

Cyber Protect is a network security simulation tool designed by the DISA [6]. It revolves around the purchase and application of information security countermeasures in a Local Area Network (LAN) environment. It takes place over four quarters. Each quarter the user makes decisions about what resources/countermeasures to purchase and put in place [7]. After making those decisions, the simulation is set in motion. The user is then subject to a variety of security attacks. The following cycle steps are repeated four times:

- First step, choose computer network security resources, e.g., user training, redundant systems, access control, virus protection, backup, disconnection, encryption, firewalls, and intrusion detection.
- Second step, applies/installs resources by drag and drop to a specific location on the cyber protect simulation dashboard.
- Third step, experiencing a variety of attacks. There are nine possible forms of attack, e.g., jamming, viruses, moles, social engineering, packet aniffers, data theft, data modification, flooding, and imitation (spoofing). The numbers and types of attacks are random; they can come from outside and inside an organization.
- Fourth step, receiving report indicating performance level. For every quarter the user receives a score sheet based upon how well they did in purchasing and applying resources to thwart the attacks.

In cyber protect simulation exercise, the user acts as an information leader within an organization. The user has full responsibility to protect or to defend his LAN department. Moreover, by utilizing cyber protect simulation dashboard, the user can freely setup the best and appropriate strategies of a LAN configurations which are expected to be immune from various types of threat, attack or data breach [8].

In order to successfully complete the simulation, meeting a "commanders" goal, the user needs to score 90 or above. As in real world situation, there is good and bad experiences and/or fortune associated with the simulation. A user might do very poorly in allocating his resources, yet through good fortune be subject to very few attacks, and therefore receive a final high score. At the other end of the spectrum, the user might do a pretty good job in allocating the resources, yet because of numerous attacks, the ending tally would not be good. Even with perfect "known" defenses, the enemy may still slip through.(see Figure 2).

Figure 2. Cyber protect simulation dashboard

The objective of cyber protect simulation exercise is to produce a minimum 90% security readiness rating. If the user achieves this requirement, then the user can print out a certificate states that the user has passed network security readiness rating as an ultimate information leader in his organization [9]. For this simulation exercise, a remark of 94% out of 100% was obtained, which is an evidence that the network security design met the standards and passed successfully.

III. THREATS, ATTACKS AND VULNERABILITIES

During the process of cyber protect simulation exercise, the user will experience several types of threats, attacks and vulnerabilities e.g.,:

- Flooding, from Internet (external), where the symptom on incident report stating “Network server and/or Router function seriously impaired, degraded or crashed”.
- Viruses, from internal network stating “Network users report odd characters, noises, tunes, and/or messages appearing on work station screens. Network operations are unusual, degraded or crashed”.
- Packet Sniffer, from Headquarters (HQ) stating “Slight degradation in time required for network information transference”.
- Jamming, from HQ stating “Network Transmissions become unreliable or unreadable due to interfering signals”.
- Social engineering attack, from internal network stating “Report of suspicious attempts by outside individuals to gain access to information”.

To deal with those threats, attacks and vulnerabilities cyber protect simulation exercises was divided into four quarter tasks, each quarter consist of at least two threat types, attacks and vulnerabilities. Every result obtained in each quarter task is displayed into a form of quarter summary reports. Useful experiences during cyber protect simulation process whereby the user can investigate any failures in his network security at the previous quarter. The user determines why controls in place did not prevent

 ISBN: 978-1-61208-475-6

threats, attacks and vulnerabilities, while making attempts to improve the network security system at the sub-sequent quarter.

IV. COUNTERMEASURES STRATEGY AND METHODOLOGY

Countermeasure strategy and methodology were needed during cyber protect simulation exercises. The user was asked to design a secure process, technology and personnel of the computer network systems, effectively and efficiently. The user can also identify residual risks of the modelled LAN. At this point, it was found that most of threats and attacks came from internal network; these are more difficult to tackle than the external ones (outsiders).

From the threat-driven approach perspective, most threats that came from insiders and outsiders (internet) can be handled effectively through a good methodology e.g., placing proper security and adequate peripherals, such as, firewalls, IDS and encryption, etc. The threat-driven approach is a methodology, a set of practices and a mindset. The primary purpose of this approach is to enable organizations to allocate the commensurate level of resources to defend their assets, to develop the inherent skills needed to support these efforts, and to align groups and teams into functional roles that will implement this approach [10]. Figure 3 shows a success countermeasure strategy for a LAN modeled configuration by developing appropiate security strategy, effectively and efficiently.

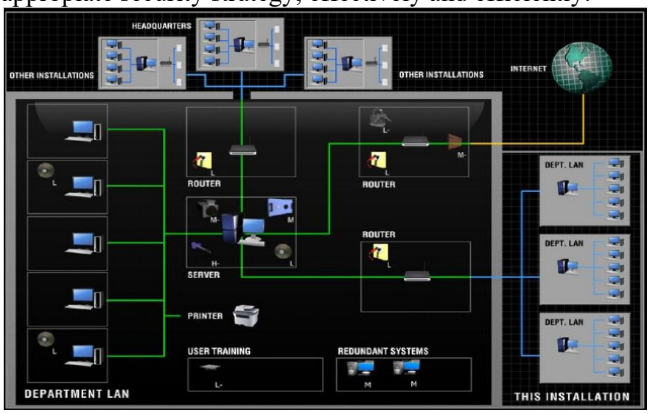

Figure 3. Design of secured LAN

It was found that the proper security strategy worked very well in the proposed modeled network security system; the strategy works as follows:

- First, configure one medium firewall and one low encryption system at the main router that is connected directly to the internet. The aim is to anticipate threats or attacks from outside the network, any kind of attacks from the Internet enter the network can be anticipated by a firewall system.
- Second, configure three low level of access control units at the entrance and exit of data communication lanes in the network to make it sure that there is no communication path that is not observed in the network. These access control units work as an early warning control system for the network administrator and it has the capability of monitoring all data transmission in the network.
- Third, complete system security in every servers with proper security equipments, e.g., high antivirus system, low level backup system, one medium Intruder Detection System (IDS) and one medium redundant system. This strategy can be applied to secure server from various attacks.
- Fourth, configure two low level backup systems on a particular client who has a high risk job in order to avoid from internal threats or breaches, especialy via social engineering attacks.

It was found that the proper implementation of countermeasure strategy is a crucial point in cyber protect simulation exercise. The countermeasure strategy might be implemented in various LAN departments, but it depends on its information security and risk management policies [11]. On the other hand, several countermeasure strategies, e.g., Defense-In-Depth Strategy by the US Homeland security or ProCurve-ProActive Defense Strategy by the Hewlett-Packard innovation center can be found on internet.

A. *Defense-In-Depth Strategy*

In October 2009, the US Homeland security developed a defense-in-depth strategy as a recommended practice in order to improve Industrial Control Systems (ICS) cyber security [12]. This strategy is not just about deploying specific technologies to counter certain risks, but it depends on how effective security program for an organization, its adherence and willingness to accept security as a constant constraint on all cyber activities.

Moreover, implementing an effective defense-in-depth strategy will require taking a holistic approach and leveraging all of an organization's resources in order to provide effective layers of protection. Figure 4 shows an overview on the key elements of a defense-in-depth strategic framework.

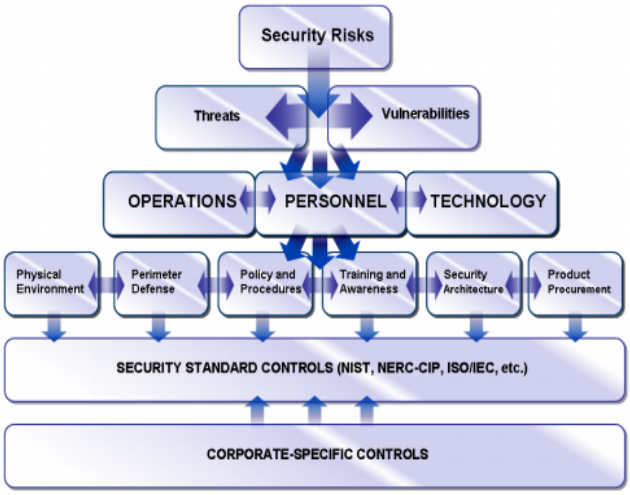

Figure 4. The strategic framework for cyber defense-in-depth

 ISBN: 978-1-61208-475-6

The basic principles of this framework are as follows:

- First, to know the security risks that an organization faces.
- Second, to quantify and qualify those risks.
- Third, to use key resources to mitigate security risks.
- Fourth, to define each resource's core competency and identify any overlapping areas.
- Fifth, to abide by existing or emerging security standards for specific controls.
- Sixth, to create and customize specific controls that are unique to an organization.

In order to implement a defense-in-depth strategy an organization will need to start at understanding its current risk. Risk for industrial control systems is best understood by knowing the threats and vulnerabilities that face an organization. The organization should undergo a rigorous risk assessment that covers all aspects to understand risk. Risk assessments are very crucial steps in defining, understanding, and planning remedial efforts against specific threats and vulnerabilities. All level areas and levels in the organization, including executives, must support the valuable risk assessments which are constantly updated at timely intervals.

B. ProCurve-ProActive Defense Strategy

In February 2007, the Hewlett-Packard (HP) innovation proposed a new alternative for network security: a comprehensive security vision and strategy that arises directly from the revolutionary ProCurve Adaptive EDGE Architecture™ (AEA). This defense strategy embraces distributed intelligence at the network edge and takes a holistic approach to an organization's or company's networking. The HP innovation declared a new security vision, called ProCurve-ProActive Defense strategy. This was claimed as the first approach that combined proactive security offense techniques with steadfast traditional defense security techniques simultaneously, at the edge of the network, where users connect.

As such, ProCurve-ProActive defense strategy is expected to change dramatically how network security is deployed from now on. ProCurve-ProActive defense strategy delivers a trusted network infrastructure that is immune to threats, controllable for appropriate use and able to protect data and integrity for all users. The three main pillars of the ProActive Defense strategy are as follows:

- Access Control, proactively prevents security breaches by controlling which users have access to systems and how they connect in a wired and wireless network.
- Network Immunity, detects and responds to internal network threats such as virus and worm attacks; monitors behavior and applies security information intelligence to assist network administrators maintain a high level of network availability.
- Secure Infrastructure, secures the network for policy automation from unauthorized extension or attacks to the control plane; includes protection of network components and prevention of unauthorized managers from overriding mandated security provisions; also includes privacy measures to ensure the integrity and confidentiality of sensitive data: protection from data manipulation, prevention of data eavesdropping, end-to-end VPN support for remote access or site-to-site privacy, and wireless data privacy (see Figure 5).

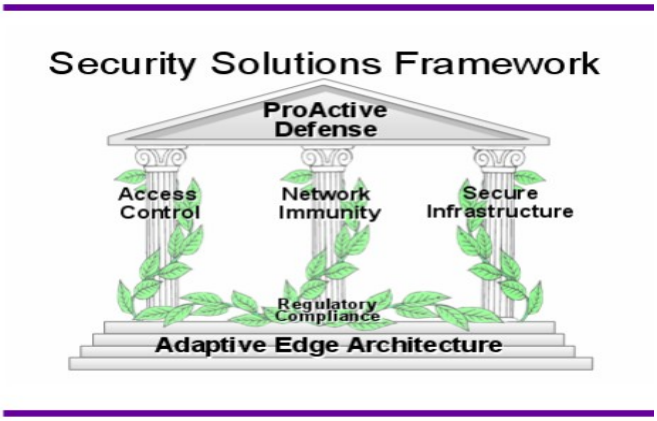

Figure 5. The Three Pillars of Access Control, Network Immunity and Secure Infrastructure

One of unique aspects of the ProCurve-ProActive defense vision and strategy is that it combines both the security offense and security defense at the same time and, most importantly, at the network edge [13]. This combined offense and defense is possible only because ProActive defense is based on AEA principles, which drive intelligence to the network edge while retaining centralized control and management. ProActive defense strategy includes characteristics such as the following:

- Additional enhancements to Identity Driven Manager, such as clientless and agent-based endpoint integrity with flexible remediation and a vulnerability assessment framework.
- Additional enhancements to Network Immunity Manager, such as increased network behavior anomaly detection (NBAD) capabilities.
- Enhanced policy control at the edge, including Web-Auth with clientless endpoint integrity authentication.
- Standards-based endpoint integrity, with trusted agent access for LANs, WANs and WLANs.

V. NETWORK SECURITY FRAMEWORK MODELS

Based on cyber protect simulation experience, organizations need to adopt an appropriate security policy as well as planning and deployment in order to enhance its network security. Every personnel within the organization, from senior level management down to the staff level, must be fully aware of the importance of enterprise information security. All employees should understand the underlying significance of security policy, planning and deployment of

 ISBN: 978-1-61208-475-6

the organization. There are several models providing security framework or security reference model, available in the market, namely the US National Institute of Standards and Technology (NIST) or the Control Objectives for Information and related Technology (CobiT) security framework, etc.

A. The NIST cyber security framework

In February 2013, the US President issued an Executive Order (EO) 13636, in order to improving national critical infrastructure cybersecurity. The EO states: "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cybersecurity environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidence, privacy and civil liberties."

This order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure (NIST 2014) [14]. NIST framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. NIST framework is organized into five basic cybersecurity activities:

- Identify (to develop the organization's understanding to manage cybersecurity risk to systems, assets, data and capabilities).
- Protect (to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services).
- Detect (to develop and implement the appropriate activities to identify the occurrence of cybersecurity events).
- Respond (to develop and implement the appropriate activities to take action regarding a detected cybersecurity event).
- Recover (to develop and implement the appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity event).

Each of the functions are then divided into categories to define more specific security practices and capabilities (e.g., asset management, access control). Subcategories describe more detailed or technical controls needed to meet objectives within each category (see Table I).

TABLE I. THE NIST CYBER SECURITY FRAMEWORK

Functions	Categories	Sub-categories	Information References
Identify	• Asset Management • Governance	• Invetory devices, systems and software, etc.	• NIST 800-53 CM-8, CA-2, etc.
Protect	• Access Control, etc.	• Review access periodically • Two-factor authentication	• ISO 27001 A6, A9, A11, A13, etc.
Detect	• Detect & Monitor for anomalies and events	• Review logs for suspicious activity, etc.	• NIST 800-53 AU-6, CA-7, etc.
Respond	• Mitigation of security events, etc.	• Report suspicious events, etc.	• ISO 27001 A6, A16, etc.
Recover	• Recovery planning, improve-ments and communi-cation	• Recovery plan • Manage public relations • Repair reputation	• NIST 800-53 CP-10, IR-4, IR-8, etc. • ISO 27001 A16, etc.

B. The CobiT security framework

CobiT is an Information Technology (IT) governance framework developed by the Information System Audit and Control Association (ISACA). CobiT consists of acquire and maintain application software; acquire and maintain technology infrastructure; develop and maintain procedures, install and accredit systems and manage changes. In April 2012, CobiT 5 was released, with the concept of enterprise governance of IT as a foundation.

CobiT 5 provides a comprehensive framework that assists enterprises to achieve their objectives for the governance and management of enterprise IT [15]. CobiT 5 brings together the five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of stakeholders (see Figure 6).

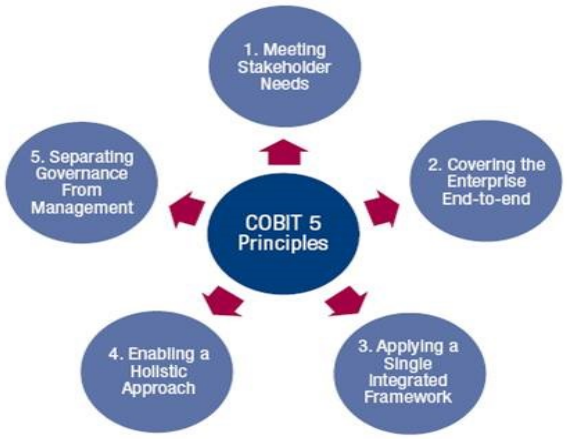

Figure 6. The strategic framework for cyber defense-in-depth

- Principle 1, meeting stakeholder needs - stakeholder needs are translated into specific enterprise, IT-related goals and enabler goals.
- Principle 2, covering the enterprise end-to-end – governance and management of information and related technology is addressed from an enterprise-wide, end-to-end perspective.
- Principle 3, applying a single integrated framework - COBIT 5 defines the overarching governance and

 ISBN: 978-1-61208-475-6

management framework that has been designed to integrate seamlessly with other good practice guidance, e.g., ISO 38500.

- Principle 4, enabling a holistic approach – the seven categories of inter-connected enterprise enablers are set out below (see Figure 7).
- Principle 5, separating governance from management. CobiT 5 advocates that organisations implement the key governance and management processes (see Figure 8).

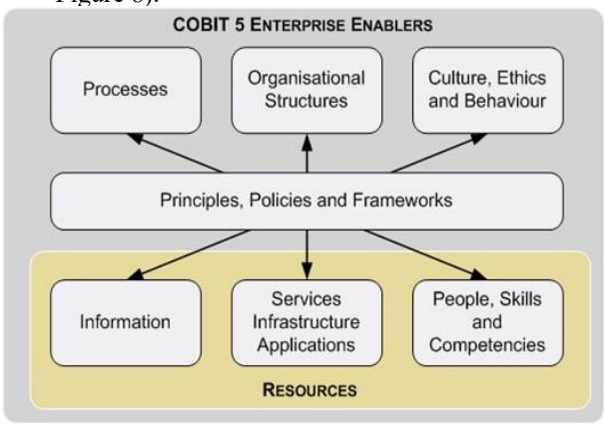

Figure 7. The seven categories of CobiT 5 enterprise enablers

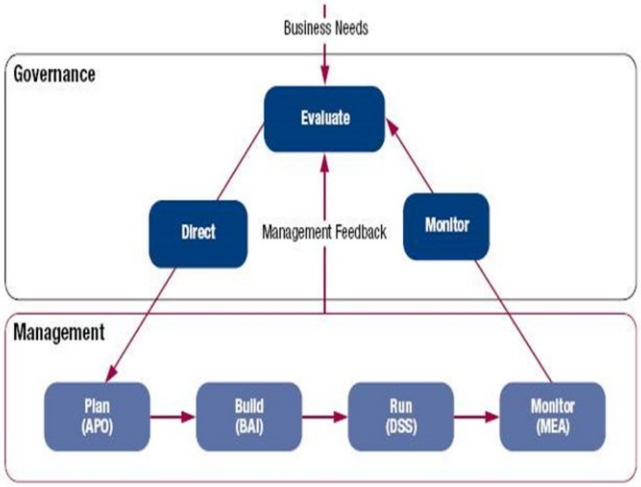

Figure 8. Separating Governance from Management

VI. CONTRIBUTION

This paper contributes an initial security framework concept, so called, The Six-Ware Framework (The SWF). The SWF concept is a comprehensive security solution to enhance an organization's network security resilience from various threats, attacks and vulnerabilities. This is an operational-level security strategy that enables to figure out the most efficient and effective actions that may lead to the success of cyber security operation [16]. The idea behind this new concept was inspired by NIST cyber security platform version 1.0., dated 12 February 2014. The SWF concept tries to elaborate NIST cyber security framework to be more practical for the operational level. The security framework disscussion can be found also in mashup web data extraction system [18].

The SWF concept contributes a common thought to understanding, managing, and expressing network security risks, both internally and externally. The SWF concept contributes increased security awareness environment within an organization where it requires internal/external risk assessment and also threat analysis policies. All levels employees in the organization, ranging from highest level to lowest level must be actively involved in the SWF concept implementation. Otherwise, they can not obtain better understanding of how threats or attacks can be carried out successfully across the entire organization.

A. The SWF enablers

The SWF enablers provide a set of activities, which consists of six main variables, sub-variables, indicators and information references (e.g., reference guidances). The SWF enablers are not only a set of checklist of actions to perform, but it presents key network security solutions to manage security risk and analysis in an organization computer network [19]. The SWF enablers comprises six main aspects, e.g., Brainware, Hardware, Software, Infrastructureware, Firmware, Budgetware (see Table II).

- Brainware or human factor, is the main aspect in network security environment. This variable becomes top list variable within the SWF concept. From network security perspective, it commonly known that human is the weakest link in information security environment. Human factor plays dominant role to enhance or on the contrary, to disrupt all efforts of existing information security wityhin an organization. Therefore, organizations must have function or position related to information security, e.g., Chief Information Security Officer (CISO). The CISO is a company's top executive who is responsible for security of personnel, physical assets, data and information in both physical and digital form. The CISO position has increased in the era of cyberspace where it becomes easier to steal sensitive company information. One of CISO's responsibilities is to conduct information security certification programs to all level employees. The intention is to produce "information security awareness employees" related to their position and function.
- Hardware, plays dominant role in handling threats, attacks and vulnerabilities. CISO has to teach all level employees how to use and treat organization's hardware devices safely and wisely. It is because a high-level hacker is not just relying on a specific technique, but still combined with the conventional attack, e.g., social engineering attack. Combination of internal risk assessment and threat analysis are extremely needed, e.g., controlling individual access into the organization's premises or facilities, locking systems and removing unnecessary CD-ROM or

 ISBN: 978-1-61208-475-6

USB thumb drives, or monitoring and protecting the security perimeter of organization's facilities, etc.

- Software, relates to utilization of software applications security which are used daily in the office, e.g., email, website, social media and other applications. High security awareness is really required because a high profile attacker will always kept on trying to infect or inject malicious emails and its attachments or invite to visit malware-infected websites. The attackers are also constantly introducing new threats although various cyber security application tools are available in the market.
- Infrastructureware, has an important role in facilitating secure organization network infrastructure, e.g., monitoring network from various threats, attacks and vulnerabilities. Nowadays, most of organizations have been highly dependent on Internet access. On the other hand, not all of employees have a good level understanding about security risks they might face in the office, where this condition is making the organization's network infrastructure more vulnerable.
- Firmware, includes documentation of an organization security strategy and policy, standard operating procedures (SOPs), business continuity plans (BCPs), network security frameworks or international security standardizations compliance to International Organization for Standardization (ISO), such as ISO 27001:2013 [18]; NIST cyber security framework version 1.0 or government security policy and strategy [20], etc.
- Budgetware, plays important and strategic role in facilitating implementation of the five-ware variables above. It is because an organization is urged to provide big enough money or sufficient budget to purchase e.g., network security application tools, patching systems, software licenses, training and education, certification programs, etc. It is highly recommended top level management must put this matter as a high level priority in order to build information security awareness. Allocating sufficient information security budget could protect the entire network system. Otherwise, they will face organization's significant financial losses, etc.

TABLE II. THE SWF CONCEPT (ENABLERS AND COMPONENTS)

Aspects	Variables	Sub-variables	Indicators	Infosec References
Brain ware	• CISO, etc.	• Security training, etc.	• Security Awareness	• CISSP, CISA, etc.
Hard ware	• Server Farms	• USB, etc.	• No compromises	• Bench marking, etc.
Soft ware	• Application	• MS Office, etc.	• No pirated Appl. etc.	• Regular updates,etc
Infra structure-ware	• Network Infrastructure	• Firewalls. • IDS. • DMZ, etc.	• No network security breaches, etc.	• Self penetration testing, etc.
Firm ware	• Security hand book	• Bussiness Continuity Plan	• Good Bussiness processes	• NIST. • ISO 27001, etc.
Budget ware	• Sufficient budget	• Buy software licenses, etc.	• Licences always updated, etc.	• Allocated budget policy, etc.

B. *The SWF component*

The SWF component works together as follows:

- Variables, organize network security fundamental aspects as enablers, e.g., brainware, hardware, software, infrastructureware, firmware and budgetware) at highest level. These variables help an organization in managing its security risk and analysis by organizing or clustering information, threats and attacks activity. Variables align with security and policy framework to reduced impact to organization quality of services (QoS) e.g., investments in human resources, planning and budgeting exercises or recovery actions, etc.
- Sub-variables, are sub-divisions of a variable closely tied to a particular (for example, brainware variable) security awareness activities e.g., "security awareness", "socialization and training", "cyber security certification program", etc.
- Indicators, are sub-divisions of a sub-variable, divided into technical outcomes. Indicators provide a set of results to achieve outcomes for each sub-variable. Indicators example (like security awareness sub-variable) e.g., "conducting security awareness training program"; "socializing and implementing security awareness culture in the company"; or "notifications from any social engineering attacks or security breaches that are being investigated", etc.
- Information References (IR), consists of network security standards, guidelines, methods and practices to achieve solutions or outcomes associated with each indicator. IR which presented in the SWF concept are illustrative and not complete. Examples of IR (like conducting security awareness training program indicator) e.g., "certified ethical hacking (CEH) course from EC-council"; "DoD information assurance awareness training"; and "Achieving ISO 27001 Certification"; etc.

The SWF component provides a set of activities to achieve specific network security outcomes, and references examples of guidance to achieve those outcomes. The SWF component is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by organization as helpful in managing the risk within organization network security environment.

 ISBN: 978-1-61208-475-6

VII. CONCLUSION AND FUTURE WORK

Cyber protect simulation is a good simulation tool, but it needs to be developed to face the growth of new variants of security threats, attacks and vulnerabilities. It provides users with useful experiences of tactical and strategical security situation awareness. The users are given the freedom to model and simulate the best strategy to defense his secured LAN configurations efficiently and effectively.

In this paper, the SWF concept can not be compared with the NIST, because it is just an initial proposal to enhance an organization's network security environment. In the future, the SWF concept needs to be developed more in-depth through further research on specific areas, e.g., determining more technically and specifically security framework variables, sub-variables, indicators and information references. The SWF concept acts as an early warning system measurement within an organization. It portraits the existing LAN security environment while finding the root cause of security loopholes. It can be concluded that to achieve a totally secure network environment is very difficult.

ACKNOWLEDGMENT

The authors would like to give high appreciation to the i-College, IRMC, NDU, Washington, DC., USA., for giving a valuable chance to attend cyber security for information leaders course in March 2015. The authors would like also to thank the Lemhannas RI and the Nuffic (Project Niche IDN 143) for its financial support so the authors can attend and submit this academic paper in the ICIMP 2016 International Conference, Valencia, Spain, May 22 to 26, 2016.

REFERENCES

[1] J. H. Saunders, "The Case for Modeling and Simulation of Information Security," National Defense University. http://www.johnsaunders.com/papers/securitysimulation.htm, last accessed April 2016.

[2] Sara Peters, "7 Lessons From The Panama Papers Leak," vulnerabilities/ threats, http://www.darkreading.com/vulnerabilities---threats/7-lessons-from-the-panama-papers-leak/d/d-id/1324976, last accessed April 2016.

[3] Swati Khandelwal, The Panama papers-Biggest leaks in History Exposes Global Corruption, The Hacker News, http://thehackernews.com/2016/04/panama-paper-corruption. html, April 3, 2016.

[4] Statista.com, "Number of files revealed in Panama Papers data leak in April 2016, by type," http://www.statista.com/statistics/531286/ panama-papers-data-type/, last accessed May 2016.

[5] Statista.com, "Number of files revealed in Panama Papers data leak in April 2016 by type", http://www.statista.com, last access April 2015.

[6] The i-college, Cyber Cecurity for Information Leaders course, "Cyber Protect Simulation Exercises," National Defense University (NDU), Washington, DC., USA, March 2015.

[7] Vicente Pastor, Gabriel Díaz and Manuel Castro, "State-of-the-art Simulation Systems for Information Security Education, Training and Awareness," IEEE EDUCON Education Engineering 2010, The Future of Global Learning Engineering Education, 978-1-4244-6571-2/10, April 14-16, 2010, Madrid, Spain.

[8] Cyber Protect Network Defense Simulation Tool, https://ndu.blackboard.com and http://iatraining.disa.mil/eta/ cyber-protect/launchpage.htm, the i-college, NDU, Washington, DC, USA, March 2015.

[9] Ann O'Brien, "Effective Learning Strategies: Cyber Protect – Learning About System Security", Wisconsin School of Bussiness, adapted from Jim Mensching, Chicago State University, USA.

[10] Michael Muckin, Scott C. Fitch, "A Threat-Driven Approach to Cyber Security: Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization," Lockheed Martin Corporation, http://lockheedmartin.com/content/dam/ lockheed/data/isgs/documents/Threat-Driven%20Approach%20 whitepaper.pdf, last accessed May 2016.

[11] Cyber Security for Information Leaders course, "Information Security and Risk Management," CISSP Textbook Reading, Chapter 3, the i-college, NDU, Washington, DC, USA, March 2015.

[12] The US Homeland Security, Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,https://ics-cert.us-cert.gov/sites/ default/files/recommended practices/Defense_in_Depth_Oct09.pdf, October 2009, last accessed May 2016.

[13] The Hewlett-Packard (HP) innovation, "ProCurve-ProActive Defense: A Comprehensive Network Security Strategy," Pro Curve Networking, February 2007, http://www.hp.com/rnd/pdfs/ProCurve _Security_paper_022107.pdf, last accessed May 2016.

[14] The National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity Version 1.0.," http://www.nist.gov/cyberframework/upload/cyber security-framework-021214-final.pdf, February 12, 2014, last accessed May 2016.

[15] ISACA,"COBIT 5 Framework: A Business Framework for the Governance and Management of Enterprise IT," http://www.isaca. org/cobit/pages/cobit-5-framework-product-page.aspx, last accessed April 2016.

[16] Chen, J., and Duvall, G., "On Operational-Level Cybersecurity Strategy Formation," Journal of Information Warfare: 13.3: 79-87. SSN 1445-3312 print/ISSN 1445-3347 online, 2014.

[17] Rudy AG Gultom, "Proposing the new Algorithm and Technique Development for Integrating Web Table Extraction and Building a Mashup," Journal of Computer science, Science Publication, NY, USA, DOI: 10.3844/jcssp.2011.129.142, http://www.thescipub.com/ issue-jcs/7/2, 25 February 2011.

[18] Rudy AG Gultom, "The Six-Ware Framework Proposal: A New Comprehensive Cyber Security Framework To Defend Your Network From Social Engineering Attack," Final Paper, i-college, IRMC, National Defense University, Washington, DC., USA, 19 March 2015.

[19] ISO, "ISO/IEC 27001: 2013, Information Technology-Security Techniques-Information Security Management Systems-Requirements,"http://www.iso.org/iso/catalogue_detail?csnumber=54 534, last accessed April 2016.

[20] Adam Quinn, "Obama's National Security Strategy Predicting US Policy in the Context of Changing Worldviews,"US Research Papaer, Project 2015, https://www.chathamhouse.org/sites/files/ chathamhouse/field/field_document/20150109ObamaNationalSecurit yQuinn.pdf, last accessed April 2016.

 ISBN: 978-1-61208-475-6