ENHANCING COMPUTER NETWORK SECURITY ENVIRONMENT BY IMPLEMENTING THE SIX-WARE NETWORK SECURITY FRAMEWORK (SWNSF)

Rudy Agus Gemilang Gultom , Tatan Kustana and
Romie Oktovianus Bura

Indonesia Defense University, Bogor, Indonesia

ABSTRACT

This paper proposes a network security framework concept, so called the Six-Ware Network Security Framework (SWNSF). The SWNSF aim is to increase a Local Area Network (LAN) security readiness or awareness in a network security environment. This SWNSF proposal is proposed in order to enhance an organization's network security environment based on cyber protect simulation experiences. Strategic thoughts can be implemented during cyber protect simulation exercise. Brilliant ideas in simulating an network security network environment become good lesson learned. The implementation for proper security strategy could secure an organization LAN from various threats, attack 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 proposal, so called the Six-Ware Network Security Framework has been introduced.

KEYWORDS

Network security environment; cyber protect simulation; cyber threats, attack and vulnerabilities; countermeasures strategy, LAN, SWNSF framework.

1. INTRODUCTION

In terms of network security environment it cannot be denied that 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 attack, e.g., network intrusions, DoS, phishing, spoofing, viruses, flooding, etc. At this point, a LAN security manager might allocate budget, spreading it for network security 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 LAN 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 network security environment issue today is the phenomenon of Panama papers where over 11.5 million files have been leaked including 2.6 terabytes of data. In the case of Panama papers leak, E-mail is the most of affected records (4,804,618 files), followed by database format (3,047,306 files), PDF document (2,154,264 files), image file (1,117,026 files), text documents

Natarajan Meghanathan et al. (Eds) : SPPR, SCAI, CSIA, WiMoA, ICCSEA, InWeS, NECO, GridCom - 2018
pp. 153–166, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81714

(320,166) and others file (2,242 files) (see Fig. 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].

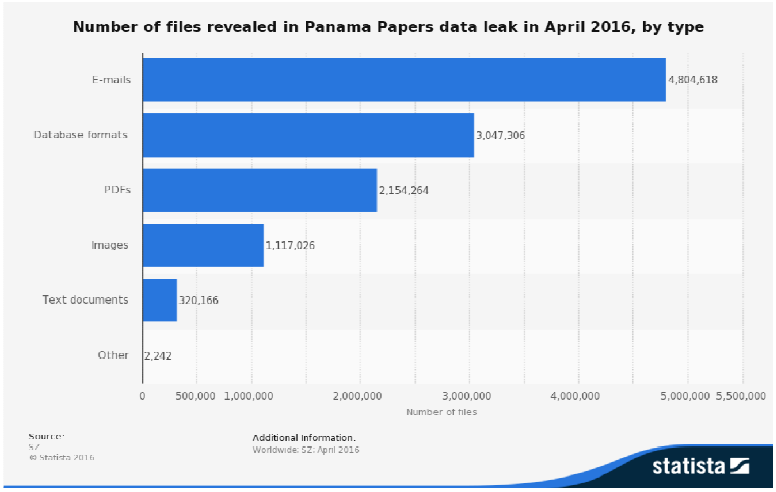

Figure 1. Number of files revealed in Panama Papers data leak in April 2016 by type, Source: Statista.com. [5]

Another good lesson learned in the context of network security environment issue today is the phenomenon of WannaCry Ransomware attack which affected companies and individuals in more than 150 countries, including government agencies and multiple large organizations globally. It was a cyber attack outbreak that started on 12 May 2017 that targeting machines running the Microsoft Windows operating systems. In Indonesia, two major hospitals were affected by this type of computer virus, they are the Harapan Kita Hospital and the Dharmais Cancer Hospital, which halted health information systems services in both hospitals as a result [6]. The affected systems had all data encrypted and a message from the attacker demanding payment of a ransom within 3 days using bitcoins or else the cost would increase. Anyone who refused to pay would eventually lose access to their files and information stored in them. WannaCry Ransomware attack is often delivered via emails which trick the recipient into opening attachments and releasing malware onto their system in a technique known as phishing.

Figure 2. Screenshot of the ransom note left on an infected system, Source: Wikipedia.com. [7]

Based on above two good lessons learned in the context of computer security, the purpose of this paper is to enhance computer network security awareness environment within an organization in order to overcome the various security threats, attack 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. This paper was inspired by the NIST network security platform version 1.0, 12 February 2014.

The rest of the paper is structures as follows. Section 2 presents the cyber protect simulation tool. Section 3 presents simulation lesson learned. Section 4 explains countermeasures strategy. Section 5 discusses why an organization needs to adopt an appropriate network security framework model to enhance its network security environment. Section 6 describes contribution of this paper by proposing an initial proposal, called The Six-Ware Network Security Framework (The SWNSF), this contribution is an early concept inspired by cyber protect simulation experiences. Section 7 contains concluding remarks and future work for the SWNSF development.

2. CYBER PROTECT SIMULATION TOOL

The Cyber Protect is a software for network security simulation tool designed by the DISA [8]. It is a dynamic learning model environment for information security countermeasures in a Local Area Network (LAN) environment. Cyber Protect has four quarters simulation steps. The user is challenged to make crucial security decision steps about what resources/ countermeasures to purchase and then try to run it [9]. Then, the simulation steps is set in motion and repeated four times where the user faces a various network attack:

- **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 attack. There are nine possible forms of attack, e.g., packet sniffers, viruses, jamming, flooding, imitation (spoofing) and social engineering attack. The attack might come from outside and inside a company.

- **Fourth step,** receiving report indicating performance level. The user receives a final score report based on how well he did in purchasing also applying simulation resources to tackle the variety of attack.

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 [10]. In order to successfully complete the simulation, meeting a "commanders" goal, the user needs to score 90 or above. But in the real world situation, the information security officers (CISO, etc.) also need a good fortune as well in order to tackle various attakcs. Even with perfect "known" security, the enemy may still find a security hole (see Figure 3).

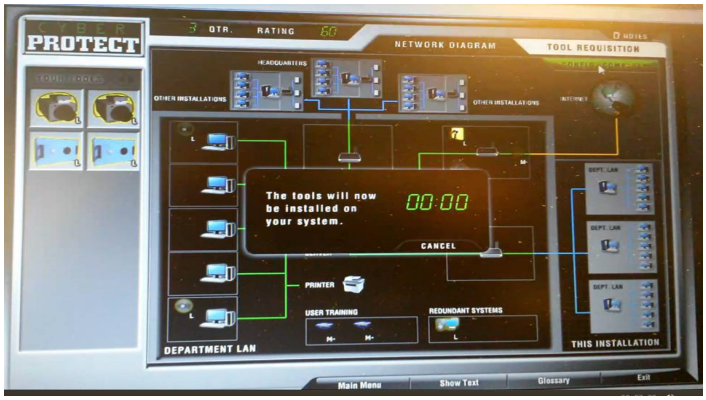

Figure 3. Cyber protect simulation dashboard

3. SIMULATION LESSON LEARNED

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

- **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, attack and vulnerabilities cyber protect simulation exercise was divided into four quarter tasks, each quarter consist of at least two threat types, attack 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 threats, attack & vulnerabilities, while making attempts to improve the network security system at the sub-sequent quarter.

4. COUNTERMEASURES STRATEGY

Countermeasure strategy and methodology were needed during cyber protect simulation exercise. 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 attack 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 proper 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. In Wikipidia, threat modeling is a process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view. Therefore, based on the behavior network model of intended functions, the user identifies and build formal models of security threats, which are potential misuses and anomalies of the intended functions that violate network security aims. [11],[12],[13].

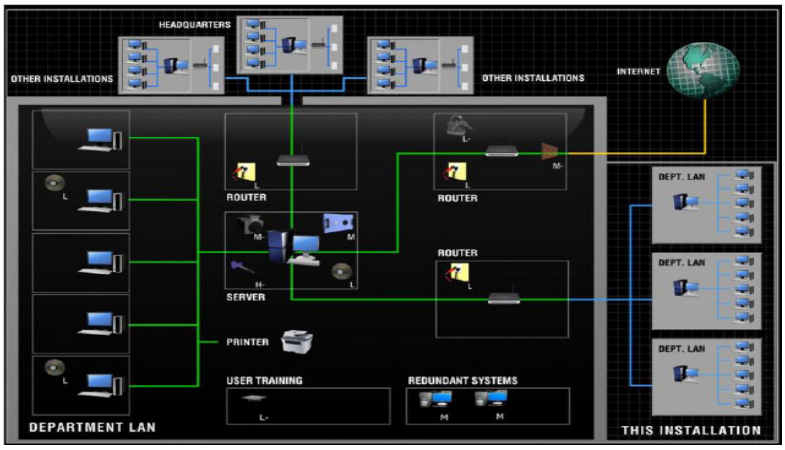

Figure 4. Design of secured LAN

Figure 4 shows a success countermeasure strategy for a LAN modeled configuration by developing appropriate security strategy, effectively and efficiently. 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 attack from outside the network. A good firewall system configuration can anticipate a variety attack from the Internet.

- **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 attack.

- **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, especially via social engineering attack.

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. On the

other hand, several countermeasure strategies, e.g., Security-In-Depth Strategy by the US Homeland security or Pro Curve-Pro Active Security Strategy by the Hewlett-Packard innovation centre can be found on internet..

4.1. SECURITY-IN-DEPTH STRATEGY

In October 2009, the US Homeland security developed a security-in-depth strategy as a recommended practice in order to improve Industrial Control Systems (ICS) network security [14]. This strategy is not just about deploying specific technologies to counter certain risks, but it depends on how effective security program for an organization in terms of accepting network security as a constant constraint on all cyber activities in the organization. Figure 5 shows an overview on the key elements of a security-in-depth strategic framework. 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.

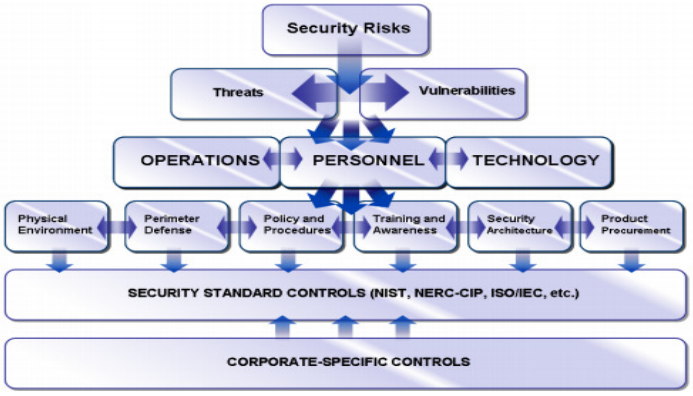

Figure 5. The strategic framework for network security-in-depth

An organization needs to understand its information security risks. It is necessary to understand and improve organizational security awareness as an integral part in implementing the strategy security protection against its sensitive information. Understanding potential threats and vulnerabilities risks is the basic security policy of 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.

4.2. PROCURVE-PROACTIVE SECURITY STRATEGY

In February 2007, the Hewlett-Packard (HP) innovation proposed a new comprehensive network security strategy based upon the revolutionary Pro Curve Adaptive EDGE Architecture™ (AEA) [15]. This security 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 Pro Curve-Pro Active Security strategy, which is expected to change

dramatically how network security is deployed from now on. Pro Curve-Pro Active security strategy delivers a trusted network infrastructure that is immune to a variety of threats/attack. It has three main pillars:

- **Access Control,** ProCurve ProActive Security strategy proactively prevent network security breaches by controlling which users have appropriate access to network systems.
- **Network Immunity,** ProCurve ProActive Security strategy is able to detect and respond to internal network threats, i.e. viruses, worms, etc., as well as to monitor the behavior and applies security information intelligence in order to assist network security officers in maintaining a high level of network availability.

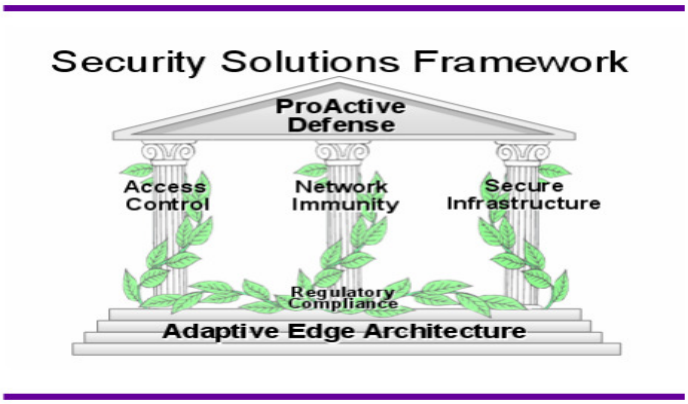

Figure 6. The Three Pillars of Access Control, Network Immunity and Secure Infrastructure

- **Secure Infrastructure.** ProCurve ProActive Security strategy secures the network for policy automation from unauthorized extension or attack to the control plane; includes protection of network components and prevention of unauthorized managers from overriding mandated security provisions. It ensures the integrity and confidentiality of sensitive data, also to protect valuable data from data manipulation or eavesdropping, end-to-end VPN support for remote access or site-to-site privacy, and wireless data privacy (see Figure 6).

One of unique aspects of the ProCurve-ProActive security vision and strategy is that it combines both the security offense and security at the same time and, most importantly, at the network edge. This combined offense and security is possible only because ProActive security is based on AEA principles, which drive intelligence to the network edge while retaining centralized control and management. ProActive security has specific strategy such as identity driven manager, network immunity manager with Network Behavior Anomaly Detection (NBAD) capabilities, policy control at the edge (clientless endpoint integrity web authentication), trusted agent access for LANs, WANs and WLANs as a Standards-based endpoint integrity.

5. NETWORK SECURITY FRAMEWORK COMPARATIVE MODEL

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 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.

5.1. THE NIST NETWORK 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". [16]. The US President EO 13636 ordered NIST to work with stakeholders to develop a voluntary framework based upon existing standards, guidelines, and practices in order to reduce cyber risks to national critical infrastructure. The NIST 2014 framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure [17]. It is composed 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 the integrity of the security plan and maintain network resilience while restoring impaired ability or services because of cybersecurity attack.

The five activities above are then divided into categories in order to determine a more specific security practices and capabilities, i.e. asset management, access control, etc. Categories are further divided into sub-categories to explain in more detail or technical controls needed to meet the goals of each category (see Table I).

Table 1. The NIST Network 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.

6. THE SIX-WARE NETWORK SECURITY FRAMEWORK PROPOSAL

This paper contributes an initial security framework concept, so called, The Six-Ware Network Security Framework (The SWNSF). The SWNSF concept is a comprehensive network security solution to enhance an organization's network security resilience from various threats, attack 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 network security operation [18]. The idea behind this new concept was inspired by NIST network security platform version 1.0., dated 12 February 2014. The SWNSF concept tries to elaborate NIST network security framework to be more practical for the operational level. The security framework discusion can be found also in mashup web data extraction system [19]. The SWNSF concept contributes a common thought to understanding, managing, and expressing network security risks, both internally and externally.

The SWNSF 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 cannot obtain better understanding of how threats or attack can be carried out successfully across the entire organization.

6.1. THE SWNSF ENABLERS

The SWNSF enablers provide a set of activities, which consists of six main variables, sub-variables, indicators and information references (e.g., reference guidance). The SWNSF 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 [20]. The SWNSF enablers comprises six main aspects, e.g., Brain ware, Hardware, Software, Infrastructure ware, Firmware, Budget ware (see Table 2).

- **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 within 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, attack 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 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 network security application tools are available in the market.

- **Infrastructure ware,** has an important role in facilitating secure organization network infrastructure, e.g., monitoring network from various threats, attack 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 Organization for Standardization (ISO), i.e. ISO 27001:2013, etc. [21], NIST network security framework version 1.0, government security policy and strategy [22], etc.

- **Budget ware,** 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 2. The SWNSF Enablers (Enablers and Components)

Aspects	Variables	Sub-variables	Indicators	Infosec References
Brainware	• CISO, etc.	• Security training, etc.	• Security Aware-ness	• CISSP, CISA, etc.
Hardware	• Server Farms	• USB, etc.	• No compromises	• Bench marking, etc.
Software	• Application	• MS Office, etc.	• No pirated Appl. etc.	• Regular updates,etc
Infrastructureware	• Network Infrastructure	• Firewalls. • IDS. • DMZ, etc.	• No network security breaches, etc.	• Self penetration testing, etc.
Firmware	• Security hand book	• Bussiness Continuity Plan	• Good Bussiness pro-cesses	• NIST. • ISO 27001, etc.
Budgetware	• Sufficient budget	• Buy software licen ses, etc.	• Licences always updated, etc.	• Allocated budget policy, etc.

6.2. THE SWNSF COMPONENTS

The SWNSF components proposed, that will be further developed as a theoretical research framework, work 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 data or information, threats and attack 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 exercise 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”, “network 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 attack 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 SWNSF component provides a set of activities to achieve specific network security outcomes, and references examples of guidance to achieve those outcomes. The SWNSF

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.

7. CONCLUSION AND FUTURE WORK

In terms of network security exercices, the cyber protect simulation is a very good simulation tool. Positively, the cyber protect simulation 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 security his secured LAN configurations efficiently and effectively. The cyber protect simulation needs to be developed to face the growth of new variants of security threats, attack and vulnerabilities. The cyber protect needs to comply with sophisticated security frameworks available. In this paper, the authors propose a new security framework, called the SWNSF concept. At this moment, the SWNSF concept cannot be compared, yet, with the NIST or other security frameworks available on the market. It is because, the SWNSF security concept is just an initial proposal to enhance an organization's network security environment.

In the future, the SWNSF concept needs to be implemented and developed more in-depth through further research on specific areas, e.g., determining more technically and specifically security framework variables, sub-variables, indicators, information references, security index scores, etc. Next step, The SWNSF concept will be implemented into a user friendly GUI (Graphics User Interface) or dashboard which acts as an early warning network security system measurement within organizations, institutions or companies. The SWNSF dashboard will work in multi-tasking environments. i.e. portraying the existing LAN security environment while finding the root cause of network security loopholes and suggest some actions to be taken to manage the security aspects. Nevertheless, at the end of the day, it can be concluded that to achieve a perfect or totally a secure network environment is a very difficult task.

ACKNOWLEDGEMENTS

The authors would like to give high appreciation to the i-College, IRMC, the National Defense University (NDU), Washington, DC., USA., for giving a valuable chance to attend the Network Security for Information Leaders (CSIL) course in March 2015. The authors would like to thank also to the Rector of the Indonesia Defense University (IDU) for supporting this strategic paper submission to the NECO 2018.

REFERENCES

[1] J. H. Saunders, "The Case for Modeling and Simulation of Information Security," National Defense University. http://www.johnsaunders.com/papers/securityimulation.htm, last accessed May 2018.

[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 June 2018.

[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, May 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 2018.

[5] Statista.com, "Number of files revealed in Panama Papers data leak in April 2016 by type", http://www.statista.com, last accessed May 2018.

[6] Two Major Hospitals in Jakarta had a massive Ransomware WannaCry Attack, https://www.cnnindonesia.com/teknologi/20170513191519-192-214642/dua-rumah-sakit-di-jakarta-kena-serangan-ransomware-wannacry, last accessed May 2018.

[7] Wikipedia.com, "WannaCry ransomware attack," https://en.wikipedia.org/wiki/WannaCry_ransomware_attack, last accessed May 2018.

[8] The i-college, Cyber Cecurity for Information Leaders course, "Cyber Protect Simulation Exercises," National Defense University (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] Cyber Protect Network Security 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. last accessed on June 2018.

[11] Michael Muckin, Scott C. Fitch, "A Threat-Driven Approach to Network Security: Methodologies, Practices and Tools to Enable a Functionally Integrated Network Security Organization," Lockheed Martin Corporation, http://lockheedmartin.com/content/dam/ lockheed/data/ isgs/documents/Threat-Driven%20Approach%20 whitepaper.pdf, last accessed April 2018.

[12] 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.

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

[14] The US Homeland Security, Recommended Practice: Improving Industrial Control Systems Cybersecurity with Security-In-Depth Strategies, https://ics-cert.us-cert.gov/sites/ default/files/recommended practices/Security_in_Depth_Oct09.pdf, October 2009, last accessed April 2018.

[15] The Hewlett-Packard (HP) innovation, "ProCurve-ProActive Security: A Comprehensive Network Security Strategy," Pro Curve Networking, February 2007, http://www.hp.com/rnd/pdfs/ProCurve _Security_paper_022107.pdf, last accessed June 2018.

[16] The US White House, Executive Order, "Improving Critical Infrastructure Cybersecurity", 12 February 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, last accessed June 2018.

[17] The National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity Version 1.0.," http://www.nist.gov/cyberframework/upload/network security-framework-021214-final.pdf, February 12, 2014, last accessed May 2018.

[18] 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.

[19] 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. Download PDF version, http://thescipub.com/PDF/jcssp.2011.129.142.pdf, last accessed April 2018.

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

[21] ISO, "ISO/IEC 27001: 2013, Information Technology-Security Techniques-Information Security Management Systems-Requirements,"http://www.iso.org/iso/catalogue_detail?csnumber=54534, last accessed May 2018.

[22] Adam Quinn, "Obama's National Security Strategy Predicting US Policy in the Context of Changing Worldviews,"US Research Paper, Project 2015, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150109 Obama National Security Quinn.pdf, last accessed April 2018.

AUTHORS

Rudy Agus Gemilang Gultom as the author is a researcher and also a senior lecturer at Faculty of Defense Technology, the Indonesia Defense University (IDU), Bogor, Indonesia. He finished his Under Graduate study (Ir.) from the Gunadarma University in Indonesia in 1991, majoring in Information Technology. He finished his Master degree (M.Sc.) in Telematics from the Department of Computer Science, University of Sheffield, United Kingdom in 1999 with scholarship from the British Chevening Award. In 2012, He finished his Doctoral degree (Dr.) in Information Technology from the University of Indonesia, Indonesia with scholarship from Indonesian Government. He can be contacted by mobile phone: +62-81380695525 or at office: 62-21-8795155562-21-87951555 ext. 7152; fax: 62-21-29618766;
e-mail: rudygultom@idu.ac.id.

Tatan Kustana as the co-author is also a researcher and also a senior lecturer at Faculty of Defense Management, the Indonesia Defense University (IDU), Bogor, Indonesia. He finished his Master Degree (M.Bus) from RMIT University of Melbourne, Australia in 1997. He also finished another Master Degree (M.A) from Deakin University, Melbourne, Australia in 2010. He can be contacted by mobile phone: +62-812943406609 or at office: 62-21-8795155562-21-87951555 ext.7001; fax: 62-21-29618766;
e-mail: tatankustana@idu.ac.id.

Romie Oktovianus Bura as the co-author is also a researcher and also a senior lecturer at Faculty of Defense Technology, the Indonesia Defense University (IDU), Bogor, Indonesia. He finished his Master and his Ph.D. studies from the Southampton University, United Kingdom in 1997. He can be contacted by mobile phone: +62-81219588063 or at office: 62-21-8795155562-21-87951555 ext.7001; fax: 62-21-29618766;
e-mail: romieobura@idu.ac.id.