Application Of Cyber Security Controls

Abstract-

This paper shows how Cybersecurity Controls makes options and regulations which every individual, partnership, corporation, company and state or federal organization have to arrange or work out in the development and stronghold of cyber-security control.

Over the past decade, it is obvious that Cybersecurity control is working out in the reduction of cyber-crime or attacks which may lead to the breakdown of an organization or self-owned business.

The center for internet security Controls (CIS) publicly supports and defend these security control, which provides a certain plan and defence protocol for the organization against developing attack with a strong structure and

ideas to provide a strong defense to detect, prevent and protect data from attacks. One of the most important advantages of the Control is that the effective ones are prioritized and focused on. In general, it rests with the scientific organization to use their full energy to improve the security control so that the internet could be safer and the internet security control (CIS) could be capable of working successfully.

Keywords: Cyber Security Controls; CIS controls, Cyber-attack, Control Analysis.

1. Introduction

Cyber-attacks are increasing more and more due to the development and creation of systems project with unprotected web interconnection wares produced by individuals or organizations in everyday life. An example is the US democratic National committee and other organizations like yahoo, Ashley Panasonic, Sony, Target, and some other government parts such as the US office of personnel management are the latest cyber-attack victims. It is always

a big danger with implications whenever there is data leaks about important and top information about users which may lead to loss of property, life and problems in critical infrastructure. (Rupinder Paul Khandpur et, nov 2007).

With these ever rapid increase in cybercrime and attack my choice is to talk more about CIS in this paper which is the main sets of controls to be executed even though there are many other sets and ways of controls made by the information technology like NIST Special, production 800-53, Revision 5 and NIST that depend on a hazard assessment. There are about 20 sets with condition like malware defense, data recovery, account observation and incident response with managing and penetration reviews. (Anon, 2017).

According to the ENISA Threat landscape report in 2013, there is a steady rise by a large number of emerging threats. In the last decade there is a comparison between ‘Emerging Threat’ and ‘Cybersecurity initiaitives’ group which is seen to be a modern cold war face-off.

This war declared is unbalanced and uneven, as we do not know how many weapons are with the attackers and how expensive, dangerous or capable the weapon may be compared to the real way from a successful attack. However, the ‘cybersecurity initiative’ need more fund in other to build a more strong defensive side, which would reduce the risk of the attack. The emerging threats don’t counteract even if the expenditure increases, turning the attacker from an ordinary hacker to a criminal causing chaos and putting the organization into a vulnerable situation or even the world behind cyber offensives and crimes. (ED Frangopoulos et).

The wide-area monitoring control are known to cover a large made up by system programs, using a provided network of intermediary devices which enable you to account, carry, solve and keep real-time program measurements. The modern power systems are totally different from the underlying information and communication technology (ICT) infrastructure that provide efforts to the operation and management.

The scientific community are meeting on how to improve the efficiency and functionality of these programs and support systems, there is always enough quality in the power system of ICT support but the lack of any of these may sometimes result to improper quality in the source of power like due to bad understanding of ICT limitations. Example is the effect of architectures on the communication performance in a situation where there is delay or failure due to the increasing communication delay in a system like oscillation damping using a SVC (static var compensator). Too much of concentration on the function of ICT over their non-functional part may trigger to the stove-pipe system. (M. Chenineet, April 2014).

In CIS about 20 controls are divided into different sub controls making the sum of 171 sub controls in total. Furthermore, there are three groups called the basic, foundational, and organizational which the twenty controls are added into respectively. In version 7 the small and moderate (medium) sized Enterprises (SMEs) are look after by the three implementation groups while the larger organization are expected to implement each of the three groups.

Ii. Related Work

The CIS control works together whenever there is an attack, they bring together people with experience and knowledge on how to create an effective defense these people might be an individual, companies or from the government with a different role such as vulnerability-finder, users, auditors, fault-finder, defender, threat-responders and analysts, programmer etc and within various areas like the government, power, defense, finance, transportation, academia, security and IT, who work together in creation, adoption and support to the internet security controls.

The best defensive techniques have been put in work to prevent or chase down the attacker by the top expert from companies using their great first-hand idea to concur cyber-attack. This shows and proved that the CIS controls are the best and effective set of methods measures that we can use to detect, prevent, respond and mitigate effect from the popular ones to the most dangerous from those attacks. The CIS controls can address detecting already-destroyed systems and avoid attackers to take actions and stopping the first compromise of the machines. The CIS also have a special group known as the IGs. They handle cut through the CIS controls stretch to different areas of enterprises and businesses. Every IG is made depending on the last one. Like the IG2 including IG3, and all the sub-controls in IG1 and IG2.

Each IG know a subset of the CIS controls society has vividly checked to be reasonable for the organization with the same risk and resources.

CIS control is an organization made up to focus on what is significant as a bottom-line for defence and cyber protection. CIS RAM described the Risk Assessment Method toward a well-organized duty of care in the sub-controls implemented by the organisation which may have to secure important information. (control, april 1 2019).

According to CIS the easiest way not to let your information security to be compromised is to eliminate all information that is no longer useful on an everyday basis. Hide and retention of information that is needed and delete it immediately they are no longer useful, this method reduce attack and save effort and enables you to detect an attack easily. There was a case whereby almost 20% of information was stolen from a company network while the victim had no clue that the data existed on the organization's network.

The rapid growth of cyber-crime also affects financial institutions. Some of the companies have launched an insurance backup which would cover the cost needed to come back after a cyber-attack, internet problem, company errors or accidental events. Furthermore, most organizations also brought up a product that focus on cyberattack analysis, assessment, client support, and risk assessment. (Bendovschi*, April 2015).

In addition, the submission of Risk assessment method(CIS RAM) is a nullification of its basic rule thus there is a movement towards other works, like the National institute of Standard Technology(NIST) establishment. The organization's top expert know how to manage and do not need a new controls that were never missed or in a confused state called "fog of more" as owned by the controls (Moore et al, 2015).

After, Dan Geer first support on Risk management logics cyber insurance has been put into academic discussion and bruce Schneier rule out is method of cyber insurance analyzing how security ideas are put in by an insurer's paperwork and the alternative insurance premium level. Likewise, CIS controls on Cybersecurity are important due to the reduction of risk vulnerability, which can run from the top to the bottom. In addition, the chief security can actualize control without the need for a risk assessment in place and risk policy is appointed to individual, which lead to no all-inclusive danger or reusable risk on cyber-attack from different organisations. There are different needs that insurers want while the policy makers of the different companies always search for protection and prevention. (Woods et al, 2017).

III Analysis and Critical Discussion.

Most Organisation has its own ("lexicon") and the internet world is the same. Devices like Computers, Smartphones, and the web are built on technology background. The more research you make individually the subject get more confusing technically but if we all work together on the subject on cyber-defense- with organization such as government, industry, companies, and business then it can help in knowing the concepts.

Security is very difficult to maintain without being damaged. Even if there is implementation in all the controls does not stop an attack but it can delay the attack due to the complexity in terms of cost, duration, experience of the attacker, strength or the fear of getting caught, arrested or

going to jail.

Whitelisting tools can be used for the implementation of whitelisting but the whitelisting tools have to be combined with policies or application execution tools that anti-virus and very fast OS (operating system). The most common and available tool today is commercial software and some asset inventory tools.

Malware code, worms, denial of service, viruses and Trojans malware, social engineering, malicious insider, phishing, spear-phishing, and stolen devices are the most popular and well-known attacks and based on research it is difficult to deduce the right number of different attacks types.

However, the results could be divided into four stages based on the motive of the attack the cyber-crime, cyber-war, hacktivist, and cyber-espionage. (Bendovschi*, April 2015).

(Andre 2017) said the lack of cooperation among health cares, hospitals and the development of medical devices leads to the rise of attack even when the safeguards are intact. Also, due to not practising adequate information technology (IT) and using vulnerable devices coupled with human failures allow attackers to get access easily into the organizations. The attack on Iranian centrifuges (worm attack) that took place in 2010 which led to the total take-over of the Siemens supervisory control and information acquisition due to lack of developed technology to detect and prevent the attack.

Insecurity control Appendix F, some security controls and control enhancement cannot be found in the lower impact baseline, because they are special controls that are used in higher baseline which can be used in maintenance of security control with the aim to protect the required level in line with the company assessment of risk. There must be enough set of security control to further mitigate danger to an organization’s operations, property, owned businesses, and the world.

However, when an organization's information system inherits two or more results in a security control it is said to be a common control. They have the higher capability in the set. There are different types of technology-based Common Control such as the public key infrastructure [PKI], access control systems, cross-domain solutions, boundary protection, and the authorized secure standard configurations for clients/servers. Security costs can be amortized within many information systems if the common control is well documented, managed, implemented, assessed and authorised. (Blank(NIST), April 2013).

Furthermore, The Internet information system(CIS) enhanced the use of audit log email, privileges, malware defenses and web protection but not knowing there is a weakness which is the biggest weakness in any organization which is the end-user. (Basharat et al, 2012) said that in many businesses and organizations administrative or operator privileges are misused, such like giving users permission to perform task,s not in their job description. These could lead to phishing, impersonation, spam emails and the spread of malicious software.

A systematic update is required to maintain a high level of cyber-security. Keeping updates become tool for repairing bugs and changing up security systems during the manufacturing phase of software (Brown 2005). It is impossible to perform a complete debugging based on the size of the code and limitations fixed on the software produced by the market considerations.

The key of any organisation is trust, as well as for security too. Security promotes the development of trust between man and technology. If we are unable to secure personal information, it will have a bad reputation for technology adoption and the whole Information communication Technology. This means, a leader is needed to face challenges around cybersecurity, self-owned business, government, and education to know we can build up the trust upon which we all depend. The lack of a leader can also put an organization at risk, someone needs to handle and give orders in an organized sector. The National Defence education Act (1958) was appointed in law in the states, with the purpose of giving money to educational institutions. Not knowing that the Americans was behind the Russian aim was to push them away to the space. Roughly $1bn was invested on science education in the last four years' durations. (ACS, Nov 2016).

50years ago, in order to confirm the attributes of systems, different scientists worked together to develop a machine suitable for the task. Showing that the defense assets results to be less challenging unlike the general perfection and considerable study owned to these testing schemes in ways of supporting the development of sound systems. One reason is that knowing the meaning of security itself is difficult and ‘brainy’. A system conforming to the Bell-Lapadula model doesn’t mean it would not lack the security properties said John Mclean who used System Z to prove it. Another developer of verification system named Don Good, in 1986 sent out an email that year: “I think the time has come for a full-scale redevelopment of the logical foundations of computer security….”. (Carl E. Landwehr, 2010).

In Addition, inappropriate management of information systems and inadequate competencies in cyber-security are the main causes of the cyber incident not by “accident” or “unfortunate”. Most ICT system has lots of inbuilt IT controls, which makes the system reliable, accurate and effective. It's very useful to know how important security control is. When you are able to detect and prevent cyber threats in a sector it reduces the chance of getting exposed to cyebr risk. (Mario Spremi? et al, july 2018)

IV. Conclusions

So far without technology the world would not be this better. Humans use the help of technology in so many activities. As we know cyber-attack cannot be eliminated but more future works are necessary to develop cybersecurity controls as enumerated by CIS controls and their usefulness. Also, more work is needed on the SMEs who have very low technology to help them fight against attacks and cyber-crimes. Every account must always be monitored very closely. If any account has not been used for a long time or is dormant this type of account must be removed and blocked from the system. Every User must verify their account before activation and they should utilize multi-factor authentication. Educating users not to leave their account on while not in use and the need for users to always log out of the system.

Finally, there should be awareness for people that do not know about cyber-attack and how they operate in the system. Cybercrime has ruined many organizations, properties, and life these is due to ignorance and low cost on the prevention of cybercrime. Free seminars and training should be available to young and old people. Whatever happens now affects the future.

References

1. ACS, Nov 2016. Cybersecurity Threat Challenges opportunities.
2. Anon, 2017. https://www.hitachi-systems-security.com/blog/benefits-incident-response-plan.. [Online].
3. Bendovschi, A., April 2015. Cyber-Attacks – Trends, Patterns, and Security Countermeasures. p. 24 – 31.
4. Blank(NIST), R. M., April 2013. Security and Privacy Controls for federal information systems and controls. pp. 800-53.
5. ACS control, C., April 1, 2019. Center for Internet Security. Volume Control version 7.
6. ED Frangopoulos, south Africa. Cybersecurity Economics: Induced Risks, Latent Costs, and Possible. p. Pretoria.
7. M. C., April 2014. A Framework for Wide-Area Monitoring and Control. Volume 29, p. 2.
8. et, R. P. K., Nov 2007. Crowdsourcing Cybersecurity: Issue Singapore, pp. 6-10.
9. Andre, t., (2017). Cybersecurity is an enterprise risk issue. Healthcare Financial Management, 1 February, p. 71. [Accessed 12 November 2019].
10. Basharat,I.,Azam,F,Muzaffar,A.W.(2012). Database security and encryption: A survey study. International journal of computer Applications, 47(12).pp28-34
11. Mario Spremi? et al, july 2018. Cyber Security Challenges in Digital Economy. In: London uk: s.n., pp. 4-6.
12. r, C. r. E. L. a., 2010. Cybersecurity: From engineering to science.
13. t., A., 1 feb 2017. Cybersecurity an enterprise risk issue. Healthcare Financial Management,. p. 71.
14. Woods,D.,Agrafiotis,I.,Nurse,J.R.C., (2017). Mapping the coverage of security controls in Cyber insurance. Available at Journal of Internet services and applications., 8(8).