Security or Breach – Enterprise to Decide

Devesh Mishra ,M.S
Technologist,
Mount Sinai Health System
Columbia University, NY, USA

Vishal Goel
Technologist, PMP, MBA,
Data Analytics Operations & Security,
Rutgers Business School

Virbahu Jain,
APICS CPIM
Solution Manager
(BlockChain, Digitization)

***Abstract*— Enterprise Security Challenges have been an ongoing discussion in the professional world at the CIO/ CISO level, but the most important question is how and what we are doing about it? Are we well informed and prepared in fighting the APT's? How effective our security layer is to identify an attack sooner than later? Before it is too late, this paper talks about some of these aspects, real-time cases and how we can equip people supporting the Data/ Security in their Organizations better.**

Keywords*— Security, Breach, CIO/CTO/CISO, Kerberos, Integrations, Mergers & Acquisitions, Divestitures, supply chain.

INTRODUCTION

Technology – A Boon or Boom? In this technology era, we talking about sending people to the moon, we talking about self-driven cars and digitization. The first thing we discuss in any organization is how can we automate activities. Whether its supply chain or financial processes, whether its Open source, robotics or blockchain. It has given great advancement and effectiveness in any organization. On the one hand, it has pioneered various digital transformation on other data breaches has accelerated at an alarming rate. A tractor is designed to deliver a high tractive effort at slow speeds, but can it carry everything? In the fast-forward world; we constantly need to move whether it is a merger, demerger, acquisition however what matters, in the long run, is; what we are leaving behind. For example- We move but personal information, the habits do not change much, so we have to be mindful when we move forward. Increased level of access, integration, mergers, divestitures presents risks and potential security compromises. We are seeing a lot of predators waiting to prey leaving an organization vulnerable to attacks.

Any security breach doesn't only affect the data or data points but the entire organization reputation and inflict lasting brand damage, resulting loss in business opportunities. We need to be cognizant of how it can impact the shareholders with their top and bottom line. Today businesses rely on multiple devices, multi-tenant software and servers, numerous vendors collaborate within our institution. We need to think cohesively taking into account the entire eco-system while designing the security fabric architecture. Every industry is different the way it operates; we need to think and act like a predator and define the boundaries and perimeters like the way we do going into any war.

According to Cybersecurity Ventures, the annual cost of cybercrime globally will rise from $3trillion in 2015 to $6 trillion by 2021. The activated hackers cell is flooding marketplace by launching various tools and services to criminals. A former consultant for the FBI cybercrime team trawled the darkest picture with the available online shopping list below. Basic malware cost is as little as $1. Figure1: Shows various list price for attack tools and services

Question is what are we doing to assess and mitigate these risks? How can we prepare ourselves better? How we can embed and tailor NIST framework within our organization and what things we need to be more careful of especially during integration.

Competition, espionage, theft, sabotage, and warfare traditionally carried out "in the field", have erupted online over the wire. State-sponsored cyber-attacks target critical infrastructure, financial systems, government agencies, political adversaries, retail and consumer databases, and the intellectual property of technology firms. These critical attack vectors include the following: advanced persistent threat; business email compromise; ransomware; social engineering in social media, insider threat, and partner compromise.

Cyber-attack is not limited to "Money" but tarnishing the image of the enterprise is getting quite common. The deficit of customers and stakeholders trust is the biggest harm an enterprise could ever have. Leaders of today need to step back and assess the need, vulnerabilities and prioritizes the defense strategy to overcome these challenges.

Today, the way hackers are evolving and exploiting the organizations and people for money and other activities, we may expect the adverse level of threats in future, it could be worse and dynamic in nature, but the forward-looking, dynamic mindset is an important factor to understand the dynamics and behaviors of such challenges. Certainly, we can rely on our partners, vendors, security team for damage control but knowing your enemy well is the best way to counter such offense. Knowing and understanding the most current threats requires an extensive research of blogs, social media feeds and other sources of information, then running the checks with internal log data.

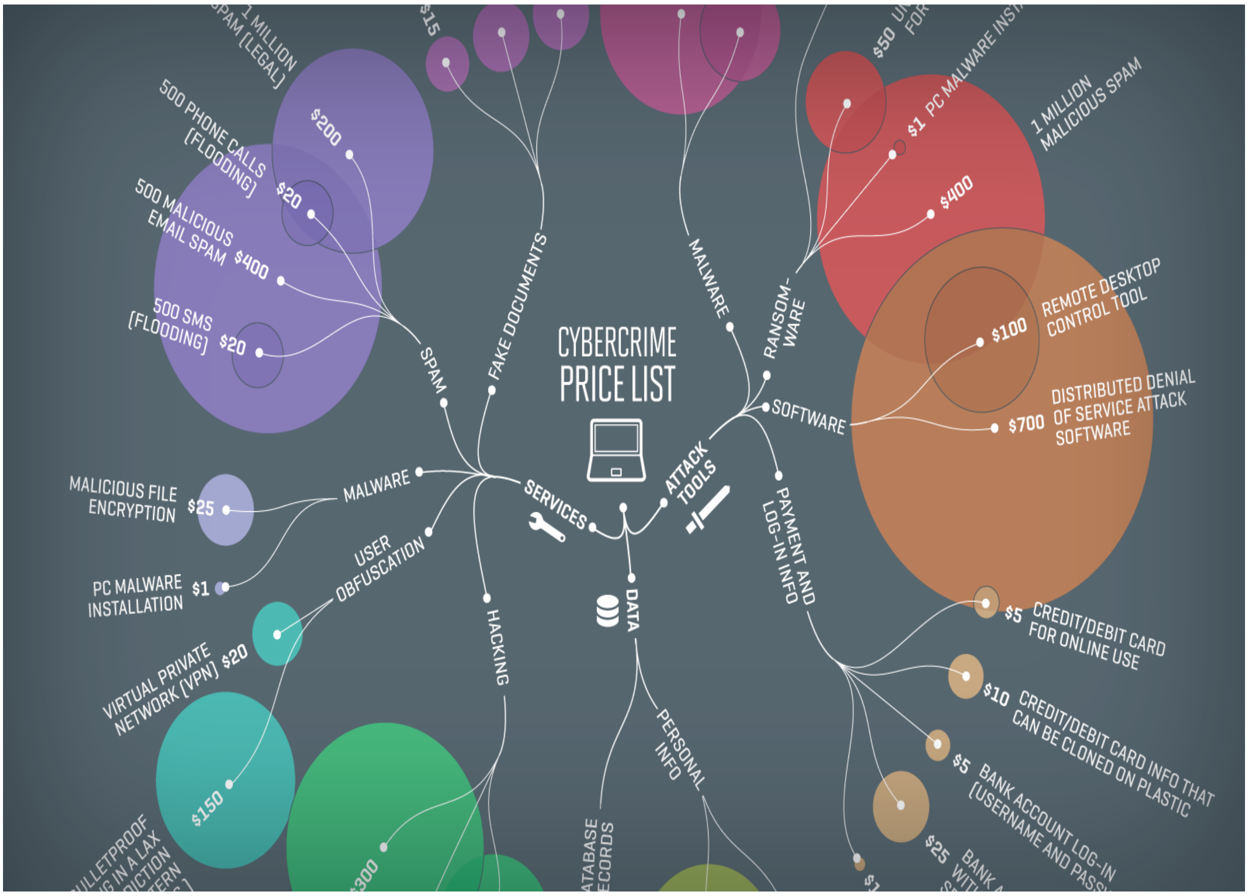

CYBERCRIME PRICE LIST
SERVICES
ATTACK TOOLS
DATA
SPAM
FAKE DOCUMENTS
MALWARE
RANSOM-WARE
SOFTWARE
PAYMENT AND LOG-IN INFO
PERSONAL INFO
HACKING
USER OBFUSCATION
MALWARE
1 MILLION SPAM (LEGAL)
$200
500 PHONE CALLS (FLOODING) $20
500 MALICIOUS EMAIL SPAM $400
500 SMS (FLOODING) $20
$15
MALICIOUS FILE ENCRYPTION $25
PC MALWARE INSTALLATION $1
VIRTUAL PRIVATE NETWORK (VPN) $20
$150
$300
$50
$1 PC MALWARE INST
1 MILLION MALICIOUS SPAM
$400
$100 REMOTE DESKTOP CONTROL TOOL
$700 DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE
$5 CREDIT/DEBIT CARD FOR ONLINE USE
$10 CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC
$5 BANK ACCOUNT LOG-IN (USERNAME AND PASS
$25 BANK

Figure1 Source: Spyware Marketplace Fortune

RECENT BREACHES

2017, World saw 45% more breaches than 2016 where the increase was 40% from prior year. The trend continues to uphill. Identity Theft Resource Center (ITRC) reported total 1,293 breaches with 174 million records compromised. Uber, Yahoo, eBay, Hyatt, Deloitte, Equifax, Anthem to name big few.

We haven’t crossed Q1 2018 but already heard about VTech paying $650k as a result of exposed personal data of 6.4million children worldwide. Jason Deli losing 2 million payment cards due to malware, Careplus, Partners Healthcare exposing 2600 patients because of malware and phishing scam, Fedex losing 119,000 personal information sitting on unsecured AWS and list goes on and on. The financial implication of any data loss is seismic; it is estimated roughly $140 per stolen record.

HIGHLY PUBLICIZED ATTACKS

•Stuxnet(2010)
•Operation Ababil(2012-2013)
•Sony (2014)
•Ukraine Power Grid(2015)
•Democratic National Committee / Hillary Clinton Campaign (2016)

Figure2: Shows the trend for the world’s biggest data breaches by the year and method of the leak based on a number of stolen records.

SECURITY FRAMEWORK – UNDERSTAND AND APPLY

This increasing trend is quite alarming. When we see some of the reasons of these breaches found 50% of them result from data hacking either due to malware, phishing, network attack, domain account malpractices and missing proper security protocols and architecture. 30% from lost media and another 20% from accidental leaked, insider job and configuration error.

One would ask if there is any silver bullet. Unfortunately, there is none. We need to start preparing now to avoid being fell prey later. Hackers are like inactive cells that enter the organization and waiting for the right time for maximum impact. There are various tools that organization can tailor themselves and prepare better. One of the most widely accepted is the NIST framework introduced in 2014 and revised to version 1.1 in 2017. This is aimed to improve the ability to identify, protect, detect and respond to the cyber-attacks Figure3. Each of the functions is further divided into category and sub-category with process standards. These functions and category can be tailored as per the organization’s needs.

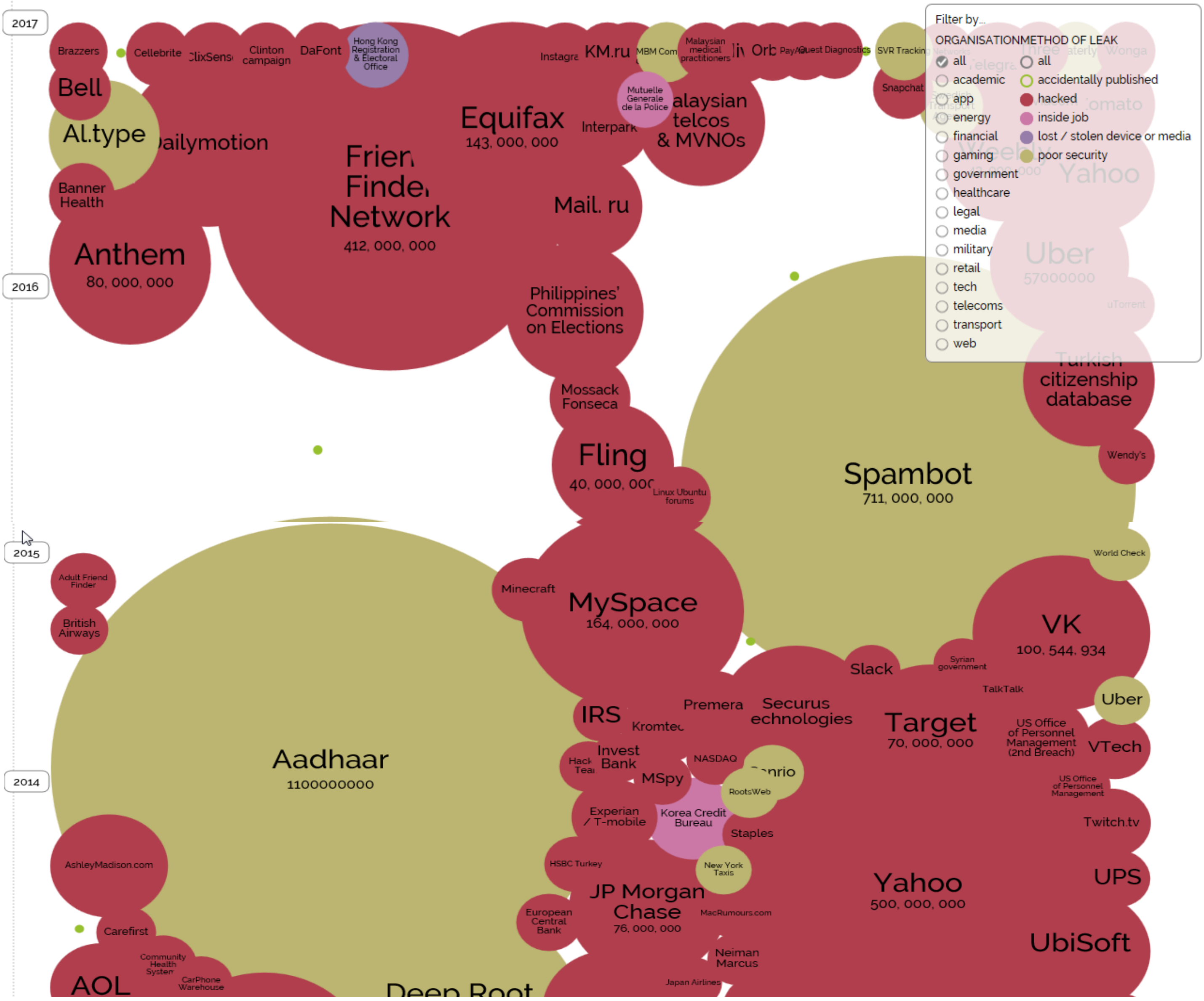


Figure2 Source: World Data Breaches 2017

The Framework is integrated into cross-domain of the business being this a supply chain, financial or human resource functions. The implementation needs to be critically designed based on the nature of the industry keeping in mind performance and cost-benefit analysis. We need to prioritize, scoping and Orient first before we analyzed the current state, future state and conduct risk and gap assessment. We need to have three lines of defense and having an alliance between risk capacity, appetite and budget (Figure 4) to support sustainable organization strategy.

Preparation and being proactive are the best tools to encounter any Attacks. There are the various steps that organization should prepare themselves before, during and after an incident and everyone from top to bottom in an organization has an equal role to play to encounter an incident.

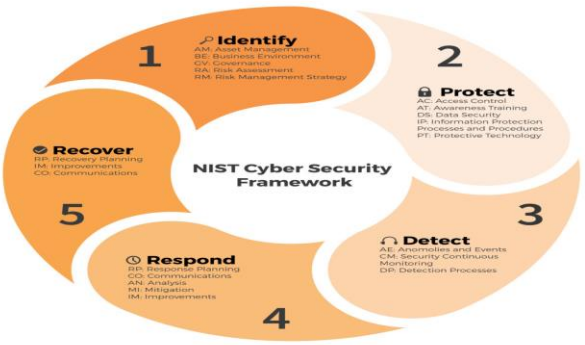
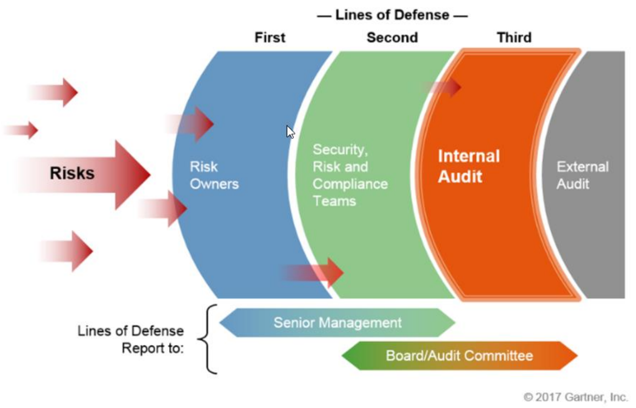


Figure3 Source: NIST



Before an Incident

- Know your enemy- Preparation is the key
- Remember your best friend-"DELETE "key
- Inventory of Authorized and Unauthorized Devices – Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network. This includes servers, workstations, laptops and remote devices.
- Inventory of Authorized and Unauthorized access – Audit the accounts across the board and terminate the access which is not being used in last 90 days.
- Inventory of Authorized and Unauthorized Software – Identify vulnerable or malicious software to mitigate.
- Secure Configurations for Hardware & Software – This applies to laptops, workstations and servers. Secure your storage servers, regularly validate and update security patch.
- Constant Vulnerability Assessment and Remediation – Proactively identify and repair software vulnerabilities reported by security researchers or vendors. Regularly run vulnerability scanning tools against all systems and quickly fix any security gaps.
- Malware Defense – Use automated antivirus and anti-spyware software to continuously monitor and protect workstations, servers and mobile devices.
- Create an incident response team (CIRT) and cyber playbook to ensure the level of communication.
- Stay relevant on the latest attack vectors and cybersecurity best practices
- Designate and engage a board committee tasked with cybersecurity responsibilities.
- Back-up and retention strategy
- Anti-Phishing behavior management for educating staffs and correcting behavior when the employee responds to phishing message.
- Threat hunting strategies to know your enemy better
- Social media policies– "What to do" and "what not to do" over the phone and social media platform.
- Deploy appropriate scanning tools for URL filtering, e-mail attachment etc.
- Ensure proper desktop and web gateway security in in place to avoid infections from malicious attachments.
- Careful review and impact of any firewall related changes.
- Identify the firm's security posture and the risks to the company/Industry
- Ensure the response plan covers communications, analysis, mitigation, and other critical tasks
- Management should develop and routinely test an incident response plan tailored to cyber security incidents. The focus should be on the organization being able to react and communicate quickly and effectively in the case of any event or incident.
- Establish a recovery plan to restore any capabilities or services impaired by a breach and to protect the company from further attacks
- Discuss with counsel whether cybersecurity risk factors in the company should be disclosed (i.e., SEC 10-K filings) in public
- Registration and validations of vendors by a secure platform like "Vendor mate" to avoid fake calls.
- Obtain liability insurance specifically covering cybersecurity risk for directors and officers as well as for the corporation
- To limit the company's liability in certain kinds of attacks, consider cybersecurity vendors certified by U.S. Department of Homeland Security's SAFETY ("Support Anti-Terrorism By Fostering Effective Technologies") Act

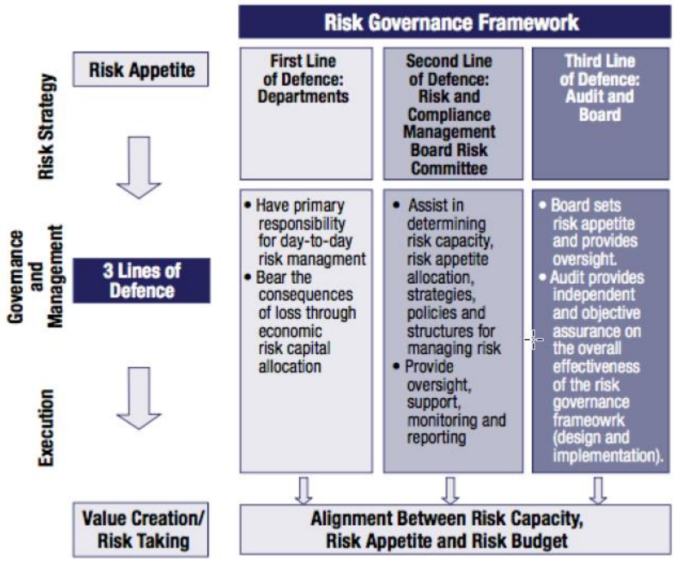

Risk Governance Framework
Risk Strategy
Governance and Management
Execution
Risk Appetite
3 Lines of Defence
Value Creation/ Risk Taking
First Line of Defence: Departments
Second Line of Defence: Risk and Compliance Management Board Risk Committee
Third Line of Defence: Audit and Board
• Have primary responsibility for day-to-day risk managment
• Bear the consequences of loss through economic risk capital allocation
• Assist in determining risk capacity, risk appetite allocation, strategies, policies and structures for managing risk
• Provide oversight, support, monitoring and reporting
• Board sets risk appetite and provides oversight.
• Audit provides independent and objective assurance on the overall effectiveness of the risk governance framework (design and implementation).
Alignment Between Risk Capacity, Risk Appetite and Risk Budget

Figure4 Risk Management of Three Line of Defense

During an Incident

- Communication is the key to address while responding to incident without losing insight.
- Briefing to shareholders or key stakeholders about the level of threats, damage etc.

- Reaching out to customers, partners, and employees about the incidents, actions and remediation plan.
- Follow-up on the remediation plan and sending the communication out until the issues are temporally resolved.
- In the case of any data loss, reach out to consumers for counselling or next steps.
- Third parties that may be required for support roles for example- forensics, crisis communication
- Communication with law enforcement agency- It is important to keep the law enforcement agencies engaged about the incidents because it is very hard to tell the level of loss of present and possible impact in future. For example- in the case of stolen data, if that data is compromised and sold to "terror organization" the possibility of disaster can't be ruled out so it's better to let the agency know about this. In addition to this, if anything changes in the future, they can refer back to the previous incidents.
- Work closely with your legal counsel and public relations team to advise C-level executives about how to disclose incident details, especially to news media.
- Stay in touch with your response team to assist as needed during response and through remediation
- Immediate involvement of law-enforcement and other agencies to avoid any further damage.
- Make sure all relevant transactions are suspended for short period of time until you validate the transactions log, network log, email server, DNS server, and AD servers to see if you could find any trace or any existing trace.
- Make sure employees are aware of such incident or any phishing email.
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Involvement of finance and purchasing department who are directly responsible for any purchase or payments, validate the approval hierarchy for better fund approval, transfer etc.

After an Incident

- After a breach has been repaired, intruders ejected, and systems restored, assist in damage control to fix the company's infrastructure and reputation
- Review incident response to assess how it went. Identify weaknesses in equipment, systems, and procedures to determine where to make improvements
- With guidance from your legal counsel, determine how to make customers whole if their data was exposed or stolen
- Consider offering free credit monitoring, issuing new account numbers, and so on. Identify the "churn rate". Counsel can advise as to any consumer remedies required by law
- Follow-up with customers and stakeholders about the next steps.
- Update the Cyber Playbook with recent activities and lesson learnt.

CONCLUSION

Cyber security is not a skillset but a mindset. Risks are dynamic in nature and dynamic mindset is essential while addressing with such situations. We certainly can't wait until something to happen but solid preparation (Known or Unknown enemy) will help us to improve our security layers and minimize the damage in case of any adventures.

CITATIONS

[1] Global Cost of Cybercrime Predicted to Hit $6 Trillion Annually By 2021, Study Says. (2016, August 16). Retrieved August 05, 2017, from http://www.darkreading.com/attacks-breaches/global-cost-of-cybercrime-predicted-to-hit-$6-trillion-annually-by-2021-study-says/d/d-id/1326742

[2] Cybersecurity Questions for CEOs. (n.d.). Retrieved August 5, 2017, from https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

[3] Fry, E. (2014, June 12). The 6 worst kinds of computer hackers. Retrieved August 05, 2017, from http://fortune.com/2013/02/26/the-6-worst-kinds-of-computer-hackers/

[4] M. (2016, October 24). 7 Types of Hacker Motivations. Retrieved August 05, 2017, from https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

[5] Enterprise Risk Management Consequence and Likelihood Tables. (n.d.). Retrieved August 6, 2017, from https://ppl.app.uq.edu.au/sites/default/files/Risk%20Consequence%20and%20Likelihood%20Table%20-%20Form.pdf

[6] Touhill, Gregory J., and C. Joseph Touhill. Cybersecurity for Executives, Wiley, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/columbia/detail.action?docID=1707094.

[7] Wheeler, E. (2011), Security Risk Management, Chapter 8, Risk Evaluation and Mitigation Strategies, Elsevier Inc.

[8] Lean-innovation-framework-to-fuel-startups, Vishal Goel, http://ems.ijert.com/download/rMQYyE4HVqFef7wTeAmkhuLtS

[9] Institute, F. (n.d.). FAIR, an international standard by the Open Group. Retrieved August 08, 2017, from http://www.fairinstitute.org/an-international-standard

[10] Deinert, A. (2016), "Cybersecurity Breach Playbook: What Every IT Administrator Needs to Know", Vantage Point Solutions, Mitchell, SD

[11] NIST. (2014, February 12) Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[12] Knock on the Door (An Analysis of Cyber Events & Forensic Investigation), Devesh Mishra , https://www.ijert.org /browse/volume-7-2018/april-2018-edition

[13] Scholtz, T., McMillan, R. (2017, January 26). Institute Cybersecurity and Risk Governance Practices to Improve Information Security. Gartner.

[14] Kark, K., Francois, M., Aguas, T. (2016, July 25). The new CISO: Leading the strategic security organization. (n.d.). Retrieved August 09, 2017, from https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html

[15] Cyber Security Guidelines for Healthcare Providers Threats and Defense from Ransomware , Devesh Mishra, IJERT , http://dx.doi.org/10.17577/IJERTV6IS120005)