World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.218

CYBERSECURITY CHALLENGES IN INDUSTRY

Akinwale Matthias Oteniya, Suxia Cui*, Yonghui Wang†

*Department of Electrical and Computer Engineering,
†Department of Computer Science,
Prairie View A&M University, Prairie View, TX USA.

Article Received on 26/04/2019 **Article Revised on 16/05/2019** **Article Accepted on 06/06/2019**

***Corresponding Author**
Suxia Cui
Department of Electrical and Computer Engineering, Prairie View A&M University, Prairie View, TX USA.

ABSTRACT

Cybersecurity has become a serious threat in our computerized society. It has evolved from cyber warfare game to catastrophic danger. As we move towards sensor level connectivity such as Internet of Things (IoT), cyber-attacks are difficult to prevent and control. Since IoT and other techniques are widely adopted in industry, cybersecurity can cripple the economy and a nation if not handled properly. The focus of cybersecurity attacks in industry is typically on high-valued assets. Targets range from power grid in energy provider, financial servers in banks, automobile industry, aviation system, health, government, military, telecommunications, education, and etc. These basically touch our everyday lives, so we cannot do without them. Security investment increases while technology development proceeds. The new reality of relentless attacks is rising at an alarming rate and new process and policies are needed to address this challenge. This paper reviews the background and suggests crucial actions to be taken in order to protect the security in industry.

KEYWORDS: Cybersecurity, Internet of Thigs, Cyberattacks, Risk Assessment.

INTRODUCTION

Cybersecurity requirement for different parastatal is unique to each, but the underlining fact or similarity is that they all need to place a high premium on the threat. Not doing so will result to serious loss of property, user information, money, and may lead to death in some cases. It is generally accepted that good data security practices ensure confidentiality,

integrity and availability of information. Cost-effective devices which used to be very expense are becoming cheaper and within reach. Digitalization increases convenience as well as security vulnerability to core systems. The number of attacks is rising and is becoming more sophisticated in the process. The recent hack of Equifax network that caused about 143 million user information being hacked is an example of the level and extent of damages our society are facing.[1] Cyber defense standard is behind the evolving threat to the economy.

The budget to protect cybersecurity is expected to rise and has been rising in the past decade. According to[2] F. Kempe, and C. Reyes, economic benefits and costs of alternate cyber future is rising dramatically. In 2009, the cost was under 30 billion dollars, and around 0.15% of the Gross Domestic Product (GDP). It rose up to over 60 billion dollars and 35% in the year of 2017.[2] Two aspects can not be ignored: 1) the capabilities of attackers; and 2) the accessibility and vulnerability of networks. Also stated by F. Kempe, and C. Reyes,[2] the Center for Strategic and International Studies (CSIS) listed the cost of cybercrime as percentage of GDP from 28 countries in 2014. The top two countries with highest percent of GDP are Germany and Netherlands. They are of 1.6% and 1.5% respectively. The United States and China immediate following Netherlands of a little above 0.6%. The two countries with lowest percent of GDP are Kenya and Japan, each of around 0.02%. According to A. Khalimonenko, and O. Kupreev[3], resources in 72 countries (vs. 80 in Q4 2016) were targeted by DDOS (Distributed Denial Of Service) attacks in Q1 2017. 47.78% of targeted resources were located in China, which is significantly lower than the previous quarter (71.60%). China, South Korea and the US remained leaders in terms of both number of DDOS attacks and number of targets, while the Netherlands replaced China in terms of number of detected servers. The longest DDOS attack in Q1 2017 lasted for 120 hours – 59% shorter than the previous quarter's maximum (292 hours). A total of 99.8% of attacks lasted less than 50 hours. The proportion of attacks using TCP, UDP and ICMP grew considerably, while the share of SYN DDOS declined from 75.3% in Q4 2016 to 48% in the first quarter of 2017. Statistics for the first quarter show that the 10 most targeted countries accounted for 95.1% of all DDOS attacks.

The above statistics illustrates how severe the situation is global wise. Among those loss, most of them are caused in industry. The challenges industries facing, resources available, as well as security issues are also different from decades ago. So this paper focuses on the cybersecurity impacts from new development and techniques towards industry.

TRENDS IN TECHNOLOGY

The world is a global village, with new technology springing up daily faster than we anticipated. Technologies are aimed to make lives better and increase efficiency in the process. These technologies have transformed the way we do things and how we interact. Different trends in the Information Communication Technology (ICT)[4] world geared towards different sectors of the economy but with one goal in mind to move society forward. The public sector has seen growth with the use of these technologies. The Manufacturing industry is able to mechanize the production unit and see an increase in profit with the introduction of robotic arms and lifts. Self-automated robots are now able to work and perform tasks without human supervision, thus reducing time and cost for the investors. Harmonization of data and information are now possible in real time with cloud-based infrastructure, which has allowed seamless connectivity and productivity across different platforms to be possible in real time.

Home security is also not left out, as it is possible for one to watch live feeds from CCTV cameras connected at home on their smart phones and computers in real time. Monetary transaction that used to depend on physical presence is a memory of the past as it is now possible to do all these transactions on any connected device. And instant transactions are confirmed in seconds. Live and online tutoring is possible at the comfort of your home or any chosen locations as long as there is connectivity. These transformations as a result of the technological trends has helped developed the society and provided easy ways of doing things. A lot of good has been brought about due to advancement in technology as it has made the world smaller and easily accessible from anywhere. We would experience even closer boundaries and more connected to virtually everything in our lives with smart devices that are capable of detecting various aspect of our environment with specialized sensors and actuators.[5] Roman Staszewski Zenseio illustrates the new generation of IoT devices with various sensors integrated in. Thus, dramatically changes today's working environment.[6] In the 70's and 80's, when personal devices were prohibited from offices, those devices were just for making phone calls, which was treated as a distraction from work. Current mobile phones are enabled with sensors, control units, and Apps to be able to assist decision-making not only to personal life, but also to work. The rules against personal devices to offices are setting loose. As employees bring their own smartphones and tablets to the workplace, there is need to create a flexible mobile environment that allows personally owned and corporate-issued devices to co-exist. IBM recently commissioned Forrester Consulting to examine the

total economic impact and potential Return On Investment (ROI) by implementing an IBM "Bring Your Own Device (BYOD)" program. According to the research done by IBM, it is observed that when employees are allowed to participate in BYOD as against total restriction, these were noticed[5]:

- There is 108% ROI over three years
- Increase in total sales of $6.8M
- More than $5.5M reduction in total mobility infrastructure and support costs
- Increase in productivity benefits of over $15K per user.

With the profit brought to the industry, several companies follow IBM to allow BYOD. Thus bring several main security concerns such as Integrity, Availability, Authorization, and Auditing (IAAA). These are essentials in gaining customers' trust. Also, there are policies and security standards such as the ISO/IEC 2700 family, which sets standards on security recommendations, requirements, risk management, and etc. These standards differ from industry to industry, but they are related.

CHALLENGES OF EFFECTIVE CYBER ATTACK DEFENSE

With more IoT devices allowed in the industry workspace, chances of getting cyber-attack increase. Cyber attackers have reinvented their skills. Always probing and looking to exploits the smallest leak in the network. Cyber-attacks occur for various reasons and at different levels. Usually these attacks are coordinated and cause more damage by doing so. There are organized groups of hackers specialized in cyber-attack and warfare. With the development in connectivity, hackers are able to proliferate from virtually anywhere using any means of connected devices to wreak havoc to any system. Some of the widely used methods in hacking include Man in the Middle Attack (MITM)[7], Denial of Service (DOS)[8], Malvertising (social engineering),[9] Unpatched Software Updates[10], SQL Injection (SQLI)[11], Cross Site Scripting (XSS)[12] and Phishing Attacks (social engineering).[13] The analysis of each attack followed by some suggestions to avoid the attacks are listed.[14]

MIMT attacks widely impact sites that require logins, such as financial sites and power grid. To avoid this kind of attack, Authentication is necessary and needs to be done when connecting to the server. This is done by use of biometrics, token key, or setting up a passphrase. Others include:

- Avoiding WiFi connections that aren't password protected.

- Paying attention to browser notifications reporting a website as being unsecured.
- Immediately logging out of a secure application when it's not in use.
- Not using public networks (e.g., coffee shops, hotels) when conducting sensitive transactions.

DOS is a form of attack performed by an attacker in order to disrupt the flow of service of an operator. The purpose of these attacks is to overwhelm a system resources such as bandwidth, CPU use, Memory or Storage in other to disrupt its availability. Companies susceptible to this kind of attack are high risk companies like financial institution, transportation, power, energy, government, manufacturing etc. DOS can be limited by putting several policies and installations in place which include: installing improved secured devices like 820.11w wireless product compatible, firewalls, intrusion detection system and mitigation systems. There are also automated systems like artificial intelligent system to aid in reducing and mitigating the attack. Creation of VLAN and VPNs also could help out.

Malvertising is a way to compromise computer with malicious code that is downloaded to the system when affected ad are clicked. An end-user is somehow tricked into running a Trojan horse program, often from a website they trust and visit often. The otherwise innocent website is temporarily compromised to deliver malware instead of the normal website coding. Cyber attackers upload infected display ads to different sites using an ad network. Some type of malware is hidden inside the ad. Enterprises can further protect themselves by not allowing users to surf the web or answer email using elevated credentials. The best way to prevent falling victim to malvertising is to use common sense and train users on security.

Unpatched Software Updates is caused by the software vendors periodically roll out software patches as soon as a bug is found. They keep maintenance on the software and try to fix it as soon as it's noticed and roll it out for downloads by their customers. These software patches are usually done to block back door access to cyberattacks by hackers. All systems running unpatched software are vulnerable to this attack and ranges from health sector, government, cooperate, and etc. The Wannacry Ransome malware attack of May 2017 was launched as an example of such software vulnerability exploit on Microsoft Windows Operating System. Keeping software up to date is very important as attackers are also exploring the same loophole to compromise the system.

SQLI refers to an injection attack wherein an attacker can execute malicious SQL statements. SQLI can also be used to add, modify and delete records in a database, affecting data integrity. Manufacturing companies with future designs and resources could be hit for their prototype being stolen. SQLI was used to breach voter's registration in 2016, Illinois, US. It can be prevented by inputting validation or codes that can identify illegitimate user inputs, use of WAF (Web Application Firewall), and etc.

XSS is a common attack vector that injects malicious code into a vulnerable web application, which put the users of the web application at risk. Thus, XSS could lead to company's reputation being collapsed due to lack of trust. Depending on the severity of the attack, user accounts may be compromised, Trojan horse programs activated and page content modified, misleading users into willingly surrendering their private data. Finally, session cookies could be revealed, enabling a perpetrator to impersonate valid users and abuse their private accounts. A web application firewall (WAF) is the most commonly used solution for protection from XSS and web application attacks.

Phishing is another form of social engineering attack aimed at attempting to deceive the user into giving up their login details and password phrases. Usually the user is lured into opening an attached email or link via messenger or email and this launches the malware by installing the malware or misdirects the user to a fake site which has been built by the attacker so as to get information or defraud the user. Financial sectors are usually attacked by phishing by creating fake websites for payment and diverting legitimate users to their website and collecting their information and possible defrauding them in the process. Antiviruses can detect phishing sites and warn about them beforehand. The best effective method is training of staffs or users on cyber security to easily detect such phishing sites with fakes URL before click it. Enabling a strong password and changing password at least twice in a year works.

ANALYSIS AND CONCLUSIONS

Setting up a suitable cyber defense in industries are hampered by numerous factors ranging from human error, policies, cost, management etc. For example, 18.8% of public sector educational finance was affected by crimeware, while more than 10% miming healthcare administrative is influenced by privilege misuse. According to Kaspersky Lab research, in the first few hours of cyber-attack, delivery company such as Fedex will be affected in US[15]; 61 NHS organizations will be disrupted in UK; and some Renault factories had to stop production in France. There is a constant war between evil and good in the cyberspace.

Widely recognized cyber-attacks can be costly to individuals and organizations, economic impacts can be difficult to measure and estimate of those vary widely. An estimated figure is above 500 billion dollars yearly with analyst predicting an increase in the future especially with the expansion in ICT through IoT and other platforms coming up.[16] Cost may be difficult to quantify but are considered to be huge. A successful attack can compromise the confidentiality, integrity and availability of an ICT system and the information it handles. Cyber theft can result in extraction of personal data, proprietary or personal information falling into the wrong hands and benefitting the attacker. DOS which slows down or completely denies legitimate users of the resources/ services provided by the organization. Botnet malware can give an attacker control of systems within an organization which can be used to cause disruption of service or equipment they control as observed in Power grids, Oil and gas and manufacturing sectors.

Cybercriminal could be categories into different needs or intent which are Monetary/extortions. Cyber attackers are continuously probing for vulnerabilities in an organization and defenders are continuously seeking ways of blocking or defending such attacks. There is a never-ending race between attackers and defenders. Vulnerabilities are abounding in an organization and usually difficult to completely seal them by the defenders. Even with known vulnerabilities and remedies are known, they may not be implemented dues to budgetary or operational constraints.

Managing the risk from cyberattacks usually involves: (1) removing the threat source like botnets, or reducing the incentives for cybercriminals; (2) addressing vulnerabilities by hardening ICT assets, e.g. updating patches, and training employees; (3) lessen impacts by mitigating damage and restoring functions like having backup resources for continuity of service for non-manufacturing industries. Security arrangement vary from establishment to establishment depending on the service rendered.

Risk identification and assessment is necessary to improving the information security of any establishment. This process must be governed by certain rules and measured against agreed upon standard. These include: (1) Assessment must meet requirements, regulations, guidance, control, recommendation and process of National Institute of Standard and Technology (NISTIR), CIP, and NAERC; (2) Complete understanding of the current cyber security framework with its current gaps, weakness, readiness and risk; (3) Building cooperation of many entities with the industry by employing a partnership approach between engineers,

operators, management and security specialty to create acceptable risks; (4) Defining minimum level of acceptable risk tolerance and create performance indicators with reasonable objectives; (5) Developing high level requirements to track cybersecurity weakness, breaches and areas of improvements.

Firewall for creating DMZs for core and critical infrastructures and limiting access is mandatory to avoid/limit attack. Firewalls have been around for years and the bad guys know how to bypass this system. It would be advisable to put up an intrusion detection system (IDS). IDS are able to detect threats within an organization with constant scanning but this also takes a long time to leverage upon. According to the survey done by Ponemon shows that, it takes an average of two months to detect and even longer to remediate. This is usually not acceptable for industrial facilities whose control systems would have been in the hands of the hacker and havoc may have been done. The use of unidirectional Security Gateway might be helpful. As these devices permit flow of data in one direction as against bidirectional of conventional Gateways. By doing so, all packets flowing in the opposite direction of the flow of the gateway device are dropped. This permit continuous monitoring of flow of data and easy identification.

Building a more secure network with use of more authentication and verification process is needed. To protect network, and interface layer, IPSEC and TLS protocol should be enabled. It is imperative to increase the level of security for all online interfaces from Adverts, information and transaction pages of the website to include a form of security. HTTPS and SSL are secured interfaces for online websites and all pages should be made to carry such protocols. Internally, the use of VLANs and VPNs to separate network traffic is crucial. Authentication and Verification of users on the internet is crucial. When authentication is sent, usually finger prints or some form of authentication should be required, not just the password and user ID. This will guard against illegitimate or compromised user logins from having access into the system.

Instituting and enforcing the right policies is key to any organization. There should be a curriculum for IT professionals and Operations Engineers with more overlap as this is required main in manufacturing industry. The gap between these two professions can be evident when there is an attack in one that could cause an adverse effect on the other. Engineers and cyber security analyst should work together to properly secure, maintain and operate critical systems within an organization. Domain engineers design and operate control

systems while cybersecurity personnel are tasked with designing, operating, maintaining cybersecurity controls for the control systems. Lack of understanding between these groups can lead to catastrophic breakdown and huge cost.

At the Management level, According to Peter Wenham, committee member of the BCS Security Forum strategic panel and director of information assurance consultancy Trusted Management. He says: "The leadership in appraising the value of data and setting the standards for handling and storing it comes from the top. If the board and senior management don't handle data properly, then why should ordinary staff do any better?"

The biggest threat to cybersecurity is the employees. The need for Structured Training and retraining of Staffs is key and necessary to minimize cyber-attacks. A well-informed staff is an asset to every company as it in turn reduces cost of cyber security because they are well informed and could act in the event of an impending attack. Once policies are properly followed and obeyed, it is easy to track down cyber-attacks and easy isolate the threat. Andrew Walls, research director at Gartner, takes this approach a step further with structured training. He says: "The traditional approach to user motivation characterized by annual training events and promulgation of security policy rarely is successful for two reasons. First, organizations do not measure the impact of training on user behavior. Second, training is treated as an externality, taking place outside of the normal stream of user activity and job responsibilities." To effectively motivate appropriate user behaviors, Walls recommends organizations should:

- Define the desired behaviors;
- Measure user compliance;
- Integrate security outcomes into staff objectives and remuneration agreements;
- Integrate security messages into normal user activities and application use.

As discussed above, there are many cyber-attacks threatened industry. Many factors need to be considered to reduce the cost. Risk identification and assessment is usually the first step towards improving the security of any industry. However, for effectiveness, this process should not be done just once. Periodic review of the risk assessment in order to identify all new potential or emerging risk and update all understanding evaluations of threats posed by previously known is the key. The frequency of such review varies from industry to industry policies. Overemphasis on the vulnerabilities in cyber-risk assessments rather than the attacks

is one of the big mistakes organizations make. The idea of updating patches alone won't make vulnerability disappear, but only reduce. There are many vulnerabilities in most industries than know bugs in software. Attack specialist are needed to be engaged in risk assessments. They should be shown the cyber security design and shown the worst-case scenarios and asked how they would attack the system to bring about havoc. Surviving the first few hours of attack is essential for fast recovery because these attacks usually follows tactics and apply latest technology to make obsolete system defenseless. Building a proactive and vigilant team who constantly look out for new threats and solutions, trainings and expertise will minimize the effect of the attacks, thus will speed up the recovery and restoration process. Post attack analysis can easily be done and necessary safe guard put in place in the event of such an attack ever occurring. Lessons learnt must be used to strengthen the defenses against future attack. To design a credible defense we need to understand what attack tools and technology our enemies are using.

ACKNOWLEDGEMENTS

The authors would like to acknowledge NSF grants #1332566, #1827243, and #1411260.

REFERENCES

1. A. Ng, "How the Equifax hack happened, and what still needs to be done," CNET, Sept. 7, 2018. https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.
2. F. Kempe, and C. Reyes, "Overcome by cyber risks? Economic benefit and costs of alternate cyber futures," Zurich Atlantic Council, Sept. 2015. https://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf.
3. A. Khalimonenko, and O. Kupreev, "DDOS attacks in Q1 2017," Kaspersky Lab, May 2017. https://securelist.com/ddos-attacks-in-q1-2017/78285/.
4. M. Singh, P. Sigh, and S. B. Sigh, "Decision Support System for Farm Management," World Academy of Science, Engineering, and Technology, 2008; 39: 346-349.
5. IBM "brings ROI to BYOD," https://www-01.ibm.com/marketing/iwm/dre/signup?source=gts-LITS-WebOrganic-NA&S_PKG=ov14067.
6. Presentation about Internet of Things Sensor Devices given by Roman Staszewski Published on Aug 31, 2016 https://www.slideshare.net/rstaszewski/iot-sensor-devices.

7. F. Callegati, W. Cerroni, and M. Ramilli, “Man-in the Middle Attack to the HTTPS Protocol,” IEEE Security and Privacy, Jan.-Feb. 2009; 7(1): 78-81.
8. NCCIC, “Understanding Denial-of Service Attacks,” Official website of the Department of Homeland Security, https://www.us-cert.gov/ncas/tips/ST04-015 June 28, 2018.
9. A. K. Sood, and R. J. Enbody, “Malvertising – ecploring web adversising,” Computer Fraud and Security, Elsevier, ISSN: 1361-3723, April 2011; 11-16.
10. M. Fisher, “The 10 biggest security breaches from unpatched software,” https://www.1e.com/news-insights/blogs/10-unpatched-software-security-breaches/ Feb. 8, 2019, retrieved online at May 13, 2019.
11. Microsoft. "SQL Injection" from https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms161953 (v=sql.105), Oct. 3, 2012.
12. J. Grossman, “The origins of Cross-Site Scripting (XSS),” https://blog.jeremiahgrossman.com/2006/07/origins-of-cross-site-scripting-xss.html retrieved online at May 13, 2019.
13. Z. Ramzan, “Phishing Attacks and Countermeasures,” In Stamp, Mark & Stavroulakis, Peter (eds.). Handbook of Information and Communication Security. Springer. ISBN 978-3-642-04117-4.
14. https://www.washingtonpost.com/news/the-switch/wp/2017/06/28/fedex-delivery-unit-hit-by-worldwide-cyberattack/?noredirect=on&utm_term=.caebc3127d27.
15. https://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid/.
16. A. Ginter, “Indiscriminate internetworking is the biggest problem facing manufacturing today.” https://www.mbtmag.com/article/2016/01/biggest-cybersecurity-problems-facing-manufacturing-2016.