CYBERSECURITY INCIDENT MANAGEMENT FOR BUSINESSES DECISION MAKERS

Mehrdad Aliasgari, Ph.D., College of Engineering, California State University, Long Beach
1250 Bellflower Blvd., Long Beach, CA 90840, Mehrdad.Aliasgari@csulb.edu

Burkhard Englert, Ph.D., College of Engineering, California State University, Long Beach
1250 Bellflower Blvd., Long Beach, CA 90840, Burkhard.Englert@csulb.edu

Tracy Bradley Maples, Ph.D., College of Engineering, California State University, Long Beach
1250 Bellflower Blvd., Long Beach, CA 90840, Tracy.Maples@csulb.edu

ABSTRACT

With incidents such as the Equifax Breach occurring with increasing regularity, it is critically important for managers and CEO's to be educated in the area of cybersecurity so that they can make appropriate decisions for attack detection, response and recovery. In this paper, we examine Equifax's handling of an incident. We then discuss best practices for incident response. Finally, we provide a brief survey of some easy-to-use cybersecurity frameworks by NIST. This work aims to educate managers of the need for a common understanding and language of cybersecurity threats so that they can successfully work with cybersecurity teams to understand and address their business' readiness, response, and recovery.

INTRODUCTION

The number of cyber attack incidents involving U.S. public and private industry has been increasing steadily. In fact, according to a report from the Identity Theft Resource Center and CyberScout [1], the number of cybersecurity incidents in the U.S. tracked through June 30, 2017, hit a six-month record high of 971. In the last two years, data breaches at Uber, Equifax, Deloitte and the U.S. Office of Personnel Management have demonstrated the wide-reaching effects of cyber-attacks affecting millions of people.

With the number of incidents predicted to rise even further, it is vital for business decision makers to play a more active role in cybersecurity. Chief Executive Officers, Chief Information/Technology Officers, Chief Security Officers must be familiar with best practices and the common technical language used in the identification of threats, protection against them, detection of data breaches, proper response and recovery from attacks. Timely incident detection along with appropriate response and recovery could have far reaching financial consequences for any organization.

In what follows, we first study the 2017 cyber incident at the Equifax Corporation. Next, we provide best practices in incident response. We then conclude with a summary of the NIST cybersecurity frameworks that decision makers at all organizations should be familiar with.

EQUIFAX DATA BREACH: A CASE STUDY

On July 29th of 2017, Equifax first discovered a cyber-attack that occurred during mid-May and July of the same year. Attackers accessed approximately 145.5 million U.S. Equifax consumers' personal data, including full names, Social Security numbers, birth dates, addresses. Equifax also confirmed that some 209,000 consumers' credit card credentials were also accessed. With millions of US consumer's private data along with hundreds of thousands of British and Canadian citizen's data stolen, this attack has been labeled by some as one of the biggest data breaches in history [2].

The attack resulted from through the exploiting of various known vulnerabilities including: unpatched Apache Struts software, unencrypted data storage, and lack of intrusion detection systems [4]. However, and more importantly, Equifax maintained an accessible online portal with direct access to consumers' sensitive data. In fact, one researcher made a report to Equifax in December of 2016 concerning the lack of access control mechanism on this web portal. Nevertheless, Equifax did not take action to close access to this portal until June of 2017, well after the breach had begun [3]. In addition, Equifax setup a website that allowed consumers to see whether they were affected by the breach by providing their personal information. However, the choice for the domain name was not ideal (equifaxsecurity2017.com). In fact, the official twitter account of Equifax published a scam URL (securityequifax2017.com) by accident and sent consumers to this fraudulent website. Furthermore, Equifax mobile applications were pulled from the Google Play and Apple App Store following the breach announcement because they did not fully utilize HTTPS and instead transmitted data in clear text after authentication [13].

Since the security breach and subsequent mismanagement by Equifax decision makers, there have been numerous lawsuits directed at Equifax. In one suit, the law firm Geragos & Geragos is seeking up to $70 billion in damages, which would make it the largest class-action suit in U.S. history [6]. In fact, Equifax is facing more than 240 class-action lawsuits and more than 60 regulatory or governmental inquiries since the incident [12]. Following the attack, the Chief Information Officer and Chief Security Officer of the company also have been replaced [8].

According to Equifax, the incident incurred $27.3 million costs in the third quarter of 2017. The total operating expenses rose 15 percent from a year earlier to $681.9 million. Under public pressure, Equifax decided to provide credit monitoring services free of charge to its customers. This has caused the company to record $56 million in liability expenses which are expected to climb to $110 million in total [12].

Rick Smith, Chairman and CEO of Equifax at the time, in a video announcement about the breach stated that "Equifax will not be defined by this incident, but rather by how we respond" [9]. It is safe to conclude that Equifax's cybersecurity practices involving this breach, from detection to recovery and response, have suffered from mismanagement at the technical, public relations and managerial levels.

INCIDENT RESPONSE

As the Equifax case study clearly demonstrates, incident response is a complex enterprise. In most cases, security incidents occur without warning. Organizations must be prepared to respond quickly and responsibly during an incident. Responses should be tailored to the type of incident encountered and it is critical to preserve evidence while not corrupting information. Therefore, a strict chain of custody should be established. The variety of scenarios facing organizations under attack is vast: an employee who appears to be the victim of malware may have downloaded the malware to hide other nefarious actions; a past employee may have installed a backdoor that allows for continuous access to your systems; an adversary may launch an attack on one part of your system only to distract you from paying attention to another part. There is no single universal response to a cyber-attack that will work under all circumstances.

In addition, when responding companies must follow all policies and laws. For example, the Health Insurance Portability and Accountability Act (HIPPA) [11] contains requirements for reporting all incidents to consumers and employees. Companies must respect employee privacy and personal rights even when there is suspected evidence on an employee's personal device.

It is critical that anyone involved with incidence response is well trained. A responder will have to inspect multiple systems and will need to be familiar with multiple technologies such as servers, routers, firewalls, intrusion detection systems etc. The responder should also be skilled with forensic technologies. Any investigation must be handled with great care.

An incidence response consists of multiple phases:

1. Initial Research: Identify the nature and impact of the incident. Develop a response plan.
2. Contain the attack by isolating systems and maintain evidence.
3. Remediate and recover from the attack. Repair damaged systems.
4. Investigate to prevent repeat events.
5. Follow up: Adjust security policy and implementation to include lessons learned.

Proper incidence response requires that a company embrace failure as part of its security effort. The NIST *Computer Security Incident Handling Guide* [5] provides a blueprint to build, classify, and measure the success of an incidence response capability. It is strongly recommended that an organization's decision makers become familiar with and adopt the above guidelines.

NIST FRAMEWORKS

In 2014, the National Institute of Technology and Standards (NIST) published a framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) [10]. This framework is meant to be used as a guide for private sector organizations to assess and improve their ability to protect and defend their cyber infrastructure. This framework describes five core cybersecurity functions: Identify, Protect, Detect, Respond and Recover. As of December of 2017, NIST has published a draft for a modified version of this framework (Version 1.1) and is accepting comments and feedback from interested companies and the Cybersecurity community. In March of 2017, the Baldrige Cyber Security Excellence Builder was published by NIST as a self-assessment tool for organizations to evaluate the effectiveness of their cybersecurity practices and identity improvement opportunities. This document leverages the Cybersecurity Framework and includes key questions for company assessment in six areas: Leadership; Strategy; Customers; Measurement; Analysis and Knowledge Management; and Workforce and Operations. Decision makers in organizations are encouraged to undergo through this self-assessment and identify improvement opportunities within their cybersecurity risk assessment and practices.

In addition, in August of 2017 and through a Special Publication (800-181), NIST published the National Initiative for Cybersecurity Education (NICE) framework [7]. This referential framework defines seven categories of common cybersecurity functions. The categories include: Securely Provision, Operate and Maintain, Oversee and Govern, Protect and defend, Analyze, Collect and Operate, Investigate. These seven functions correspond directly to the five core cybersecurity functions defined in the Cybersecurity Framework. The NICE framework then divides cybersecurity into thirty-three detailed areas and describes fifty-two Knowledge, Skills, and Abilities (KSAs) and Tasks. An effective and efficient cybersecurity team needs to possess these KSAs in order to perform the cybersecurity tasks.

THE NICE framework can be used to identify the KSAs required by an organization's cybersecurity team. Once the KSA gaps are identified, the decision makers can use this common lexicon to improve position descriptions of the necessary positions. The KSAs can guide the leaders in making hiring decisions. New positions should be developed so that cybersecurity teams can perform the tasks defined in the NICE framework and develop appropriate trainings for new hires. These KSAs will demonstrate career and promotion paths for the current and future cybersecurity workforce.

Therefore, it is imperative for CEOs, CIOs and the CISOs to become educated about the common Cybersecurity terminology. This common language allows decision makers to understand the cybersecurity team more accurately. The NICE framework can help in recruiting, retention, and training of an effective cybersecurity team.

CONCLUSION

Major organizations are under constant risk of cyber-attack. Security breaches have caused financial and public relation damages to companies. Examination of the 2017 cyber incident at Equifax has revealed mismanagement of the breach at technical, public relations and managerial levels. The incident and Equifax's handling of it have affected millions of Americans and their finances and have brought hundreds of lawsuits, regulatory inquiries, great financial cost, dropped share values and more importantly, loss of consumers' trust in the company.

With an ever-growing volume of cyber incidents, it is vital for decision makers to be familiar with best practices in data breach identification, protection, detection, response and recover. The National Institute of Standards and Technologies has created several frameworks for cybersecurity defense, incident handling and recruiting. This paper discusses some of the frameworks that should be utilized by company decision makers. Cybersecurity drills are also recommended for all organization. The drills can be used as part of an assessment of the organization's readiness for incident detection, response and recovery. Assessment is also important to evaluate cybersecurity awareness and culture among both employees and consumers.

REFERENCES

.[1] Identity Theft Resource Center, 2017 Mid-Year Data Breach Report Press release, available at: https://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release (retrieved January 27th, 2018).

[2] Charipar, V., The end of the cloud is coming, available at https://venturebeat.com/2017/11/04/the-end-of-the-cloud-is-coming/ (retrieved January 27th, 2018).

[3] Franceschi-Bicchierai, L., Equifax was warned, available at https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning (retrieved January 27th, 2018).

[4] Gallagher, S., Equifax hackers stole data for 200K credit cards from transaction history, available at https://arstechnica.com/information-technology/2017/09/equifax-hackers-stole-data-for-200k-credit-cards-from-transaction-history/ (retrieved January 27th, 2018).

[5] Grance T., Kent K. & Kim B. Computer security incident handling guide. NIST Special Publication. 2004 Jan;800(61):11.

[6] Mills, C., Equifax is already facing the largest class-action lawsuit in US history, available at: http://bgr.com/2017/09/08/equifax-hack-lawsuit-class-action-how-to-join/ (retrieved January 27th, 2018).

[7] Newhouse W, Keith S, Scribner B, Witte G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, *NIST Special Publication* 2017, 800 (2017): 181.

[8] Shaban, H., Two Equifax executives will retire following massive data breach, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/09/15/two-equifax-executives-will-retire-following-massive-data-breach/ (retrieved January 27th, 2018).

[9] Smith, R., Equifax will be defined not by this incident but by how we respond, available at: https://www.youtube.com/watch?v=bh1gzJFVFLc (retrieved January 27th, 2018).

[10] Stine KM., Quill K. & Witte GA., Framework for Improving Critical Infrastructure Cybersecurity. 2014 Feb 19.

[11] Summary of the HIPPA Security Rule, available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (retrieved January 27th, 2018).

[12] Surane, J., Equifax is haunted by its costly cyber attack, available at: https://www.bloomberg.com/news/articles/2017-11-09/equifax-haunted-by-cyber-attack-as-costs-jump-lawsuits-abound (retrieved January 27th, 2018).

[13] Weissman, C., Why Equifax yanked its apps from Apple and Google last week, available at: https://www.fastcompany.com/40468811/heres-why-equifax-yanked-its-apps-from-apple-and-google-last-week (retrieved January 27th, 2018).