Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)

ISSUE (14), Nov (2018)

www.mescj.com

Critical Elements of Response and Recovery From The Cyber Security Incidents

Dr. Abdelrahman Karrar, Mohammed Saif, Aisha Albadrany
Kingdom of Saudi Arabia, Madinah
Taibah University
College of Computer Science and Engineering
Department of Information System
akarrar@taibahu.edu.sa , mohdya12@taibahu.edu.sa, aishaalbadrany@taibahu.edu.sa

Abstract :

Cyber security are processes, strategies and plans which are employed in safeguarding internet connected systems, software and data and hardware from cyberattacks. In IT (information technology) incidence response is the systematized approach which is followed to address and manage the aftermath of a cyber-attack or a security breach. Additionally, disaster recovery (DP) is a security planning area which aims at protecting an organization from various effects of adverse events (significant). In various enterprises and all levels of organizations, there is a growing concern on these cyber-attack incidents because when they occur, they can cause a lot of damage to the companies because they produce a significant breach on privacy elements of the organization.

Information technology faces a major problem in safeguarding their data because of disgruntled employees or intentional data leaks from misplaced laptops or other data storage devices. The priority of incidence response and disaster recovery in cyber security is to contain and recover from risks so that the possibility and recovery of cyber losses are mitigated and avoided effectively. As a result, it is essential to stay informed and diligent about breaches and hacks which might occur in organizations. When a cyber threat incident is discovered, it is essential to ensure that the proper process of reporting the attack is taken. Indeed, both incidence response and disaster recovery processes should sequential, and they should be carried out in a parallel manner.

Keywords-- Cyber security, Software, Cyber threat, Information technology, Security breach, Disaster recovery, Ransom ware, CSIRT (Computer Security Incident Response Team), IRP (incident response plan), cloud computing and firewall

i. INTRODUCTION

Cyber security is processes, strategies and plans which are employed in safeguarding internet connected systems, software and data and hardware

from cyberattacks [10]. In computing, cyber

security involves the protection against computerized systems including unauthorized access to data [9]. Co-ordination or efforts in an information system is critical in ensuring cybersecurity . In IT (information technology) incidence response is the systematized approach which is followed to address and manage the aftermath of a cyber-attack or a security breach[15]. Notably, it is also known as a security incident, a computer incident or IT incident[12]. However, the goal of incident response is to ensure that situations are handled with the least damage at a reduced cost and recovery time[2].

CSIRT (computer security incident response team) conducts incidence response in an organization[5]. Complying with IRP (incident response plan) is crucial during incidence response[15]. Additionally, disaster recovery (DP) is a security planning area which aims at protecting an organization from various effects of adverse events (significant). Indeed, it allows an organization to resume quickly or to maintain mission-critical functions after a disaster[10]. However, disaster recovery enables businesses to continue operating in a normal or close to normal[9]. It is a process which includes both planning and testing though it may be involving separate physical sites where operations are restored[6]. As a result, this article describes critical elements in cyber threat incident response and disaster recovery process.

ii. GOAL OF THE PAPER

Incident Response and Disaster Recovery in IT
In today's highly connected world, cyber incidents happen on a daily basis. For instance, every corporation from the very large to small and medium companies need an incident response team. This paper describes critical elements of incident response and disaster recovery and the basic plan of operation after a cyber incident. The major goals of the research is to identify that which assets are being protected and who needs to be on the incident response team? The goal is to also identity the process for reporting or detecting an incident. It will also study the risk management and policies that are required. The aim is to find out the best practices exist for the industries. Data securing has some challenges that can reduce the efficacy of data security therefore the goal is to understand and elaborate the challenges in securing data and they ways how the data can be prevented from the security attacks.

iii. CYBER THREAT INCIDENT RESPONSE

Diverse tools such as ransomware, malware, exploit kits amongst other methods are used by hackers to perform a cyber-attack operation[15]. In various enterprises and all levels of organizations, there is a growing

concern on this cyber-attack incidents because when they occur, they can cause a lot of damage to the companies because they produce a significant breach on privacy elements of the organization[6].

I. ASSETS PROTECTED

Data is the primary asset stolen in cyber-attacks thus becoming the most protected asset. However, cyber threats can be conducted after a cybercriminal accesses a network or a computer to take some or all of the local files[9]. In this case, the other most protected items include the machines and the systems [15].

II. THE COMPOSITION OF THE CYBER-ATTACK INCIDENCE RESPONSE TEAM

The significant critical people in the CSIRT (Computer Security Incident Response Team) are experts in monitoring the intrusion of firewalls, sensors and any other security devices from the MSSP (managed security services provider). With proper management support and funding the CSIRT plays a critical role in because it provides business intelligence and risk[13].

III. PROCESS FOR REPORTING A CYBER THREAT INCIDENT

The first step of reporting a cyber threat incident is mobilizing the CSRT team . In this case, the relevant stakeholder groups which include the technical side of investigating the breach and the employee and HR representatives who are affected by the breach are notified[3]. The intellectual property, data protection, and public relations representatives' experts are informed[16]. Moreover, external representatives such as the legal teams and incapacitated internal teams should also be alerted[5].

Thirdly, a thorough investigation is conducted to determine the facts surrounding the breach[12]. If a potential employee is involved in the violation, applicable labor laws are considered, and then HR representatives consulted[11]. Conclusions of investigations are reviewed and appropriate notice and training given to the employees[6].

The fourth step is managing public relations[12]. When customer data is lost, the management should announce the details of the breach to the public. Last but not the last, the company incurs the liability of the cyber threat incident, and this could be non-legal liabilities which occur due to theft, blackmail attempts amongst others[4].

IV. CYBERSECURITY POLICIES WHICH SHOULD BE IN PLACE

Some of the guidelines included in the cybersecurity policy include the guidelines on password requirements, email standards and the handling of sensitive data [9]. Besides, some of the other essential guidelines in these policies include the instructions on when to lock computers and devices and the handling of removable computer devices[1]. Moreover, others include the handling of technology within the organization and internet and social media access standards not forgetting to mention the management of incidents especially on the procedure of responding to cyber incidents[13].

V. RISK MANAGEMENT NEEDED

An organization has to determine the assets which have to be protected[2]. As it is pointed out by the NIST (National Institute of Standards and Technology), there is no particular size which fits the solution[5]. Assets such as customer and corporate data should have additional protections. It is recommended to use the

Capability Maturity Model approach which has five levels which include the initial, repeatable, defined, managed and optimized levels[2]. Among the other most features of risk management, others include risk mitigation, consideration of the human element and reinforcing the incident response team amongst others[3].

VI. BEST PRACTICES

In 2016, India had 53,871 cases of cybercrime as recorded by the National Crime Records Bureau. One of the basic practices is that security should be put at fore[6]. The workforce should be encouraged to build and use systems or products in such a manner that the likelihood of cyber-attacks is reduced[11]. The wireless internet used should be secure not forgetting to enable the multi-factor authentication[16]. Secondly, cybersecurity should also be incorporated into the organization's risk management strategy[12].

Moreover, the cyber security incident response team should be adequately trained to follow the best protocol and practices for mitigating a cyber threat incident[6]. Besides, running numerous drills and simulations is also an essential practice towards cybersecurity [14]. Notably, estimating the sheer amount of data collected by an organizations system is critical in placemaking data within the system[4]. On the other side, compartmentalizing data in the organization and restricting access using passwords, OTPs, and multifactor authentication is also another best practice in the cybersecurity industry. Establishing a BYOD policy, devising an adequate contingency plan and the spirit of evolving with new software's is also necessary[16].

iv. DISASTER RECOVERY

Challenges in Securing Data

I. TARGETED CYBER ATTACKS

Most cyber-attacks are carried out by well-organized global cybercrime syndicates [3]. The nature of attacks is always changing because the character of the crime since the hackers do not need to meet and carry out the attack but easily communicate through the internet when they are located in different parts of the globe quickly[9].

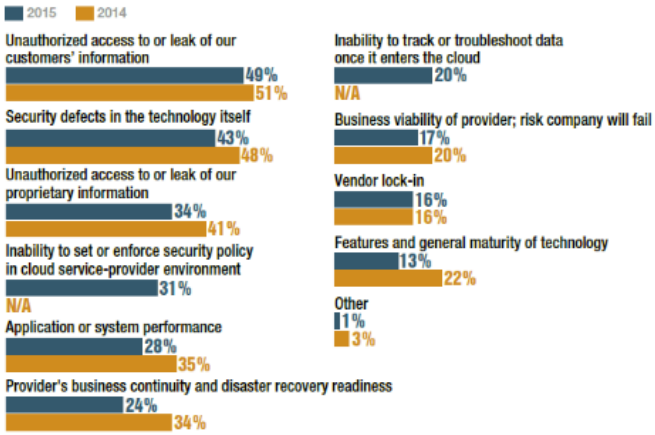
II. DATA BREECHES

Businesses face a major problem in safeguarding their data because of disgruntled employees or intentional data leaks from misplaced laptops or other data storage devices[3]. According to research, most data leaks come from within the organization[5]. As a result, the companies must be more vigilant regarding who is accessing their data especially when it comes to co-operating networks which are conducted outside the firewall[11].

III. CLOUD COMPUTING

It is hard for a business to operate without cloud computing in the process of storing information about the company. Practicing cloud computing gives rise to new sets of data something which introduces new concerns about data security[6]. It is because a business must relinquish the control of its information and data to the third-party during cloud computing[13].

www.mescj.com

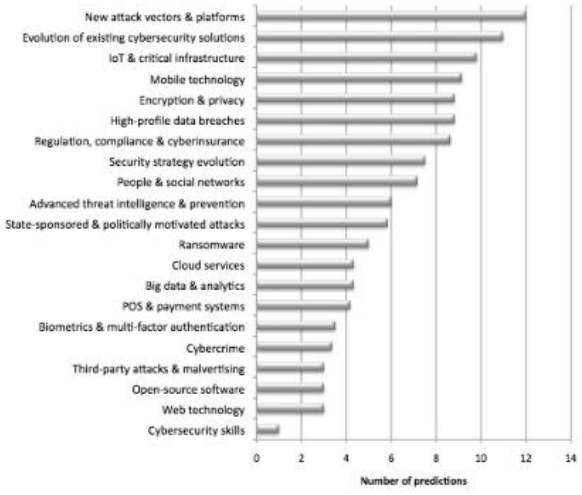


Source: [15]

Figure 1risk associated with cloud computing

IV. SOCIAL NETWORKS

Almost all employees are on different social media platforms such as Twitter, Facebook, Myspace and Instagram amongst others[10]. Most of these employees are not only wasting time on the networking sites, but they also indulge in some conversations which make them share business information on the same platforms[15]. When this occurs, the direct recipient or the other people sharing the same platform can be a threat to a business when they access the information[3]. In connection to this, it has been challenging for different companies to secure their information and data because it is difficult to constantly monitor employee social networks[9].



Source: [16]

Figure 2 Chart presenting the challenges

V. MOBILE DEVICES

The use of smartphones is ubiquitous in various workplaces. Smartphones are the most widely used networking personal gadgets[14]. They are capable of sharing extensive information and data within a short period in a secretive manner. As a result, employees are capable of downloading company's information and sharing it without any noticeable alarm[9]. Since it is not easy to police the smartphones, IT administrators in many businesses are facing very hard when addressing different matters connected to data security within the organization[14].

v. WAYS OF PREVENTING DATA SECURITY ATTACKS

I. CREATING INTERNAL POLICIES

In most cases, employees' nature and actions create the major flaw through which business data and information land in the wrong hands [5]. As a result, the firm must ensure that it implements effective policies which control and prevent employees from leaking company's information to the outsiders . Besides, the company should check and monitor people who install the business servers to make sure that the right protections are considered[16].

II. KEEPING COMPUTERS UPDATED

Companies are supposed to make sure that the entire computer network used in the firm is up to date . As a result, it is expected to pay attention to all notifications which regard updating of the operating systems used by the enterprise [5]. It is because updating these programs such as firewalls and web browsers, antivirus software and the others help in safeguarding the system from cyber threats[9]. However, ignoring them weakens the defense system of the business computers[15].

III. LEARNING FROM MISTAKES

A business should be observant and learn from its environment . In this case, it is supposed to learn and hence set the appropriate security measures before the danger strikes[14]. It is a good measure because it can protect huge financial loses which can be incurred after the attack [15]. Besides, more informed decisions should be made to safeguard any hacking issues. Other methods of preventing cyber threats and attacks include the use of cloud services, increasing employee awareness, creating strong passwords and changing them frequently and hiring security experts to work for the firms[10].

vi. SOLUTION

CSIRT teams should always be ready to respond to cyber threat incidents [3]. It is critical to ensure that the proper plan, methods and strategies of incidence response and disaster recovery both mentioned and unmentioned in this paper are employed when responding to cyber threats [11]. When a cyber threat incident is discovered, it is also essential to ensure that the proper process of reporting the attack is taken .

CONCLUSION

Cyber-attacks issues affect the entire business inclusive of all teams in the organization . Besides, it is not just a technical issue but also an operational issue[14]. However, the process should be sequential, and it should be carried out in a parallel manner at the initial aftermath of an incident[12]. However, the priority of reporting a cyber threat is to contain it so that the risks involved are mitigated to avoid any further loss of damage or data[16]. It is essential to stay informed and diligent about breaches and hacks which might occur in organizations[1]. Generally, the CSIRT should always ensure that it protects all company information with encryption[6].

REFERENCES

1. Aoyama, T., Naruoka, H., Koshijima, I., Machii, W., & Seki, K. (2015, May). Studying resilient cyber incident management from large-scale cyber security training. In *Control Conference (ASCC), 2015 10th Asian* (pp. 1-4). IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/7244713/
2. Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717-723. Retrieved from https://www.sciencedirect.com/science/article/pii/S026840121500078X
3. Ab Rahman, N. H., & Choo, K. K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45-69. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404814001680
4. Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management*, *51*(1), 138-151. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0378720613001171
5. Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., &Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy*, (5), 61-67. Retrieved from https://www.computer.org/csdl/mags/sp/2014/05/msp2014050061-abs.html
6. Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing*, *9*(1), 138-151. Retrieved from https://ieeexplore.ieee.org/document/7299312/
7. Magrabi, F., Liaw, S. T., Arachi, D., Runciman, W., Coiera, E., & Kidd, M. R. (2015). Identifying patient safety problems associated with information technology in general practice: an analysis of incident reports. *BMJ Qual Saf*, bmjqs-2015. Retrieved from https://qualitysafety.bmj.com/content/early/2015/11/05/bmjqs-2015-004323.short
8. McCann, Stephen, and Michael Montemurro. "Methods and apparatus to discover authentication information in a wireless networking environment." U.S. Patent No. 8,943,552. 27 Jan. 2015. Retrieved from https://patents.google.com/patent/US8943552B2/en
9. Manning, K. (2015). *8 Ways Businesses Can Prevent Cyber Attacks*. [online] business2community.com. Available at: http://www.business2community.com/cybersecurity/8-ways-businesses-can-prevent-cyber-

attacks-01251164#i2OQARYWHkL075qH.97 [Accessed 24 Sep. 2017]. Retrieved from https://www.business2community.com/cybersecurity/8-ways-businesses-can-prevent-cyber-attacks-01251164

10. Panko, J., & Panko, R. R. (2015). *Business data networks and security*. Pearson Education. Retrieved from https://dl.acm.org/citation.cfm?id=2789641
11. Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., ... &Haustein, M. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications*, *34*, 166-182. Retrieved from https://www.sciencedirect.com/science/article/pii/S2214212616300576
12. Tarafdar, M., DArcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. *MIT Sloan Management Review*, *56*(2), 61. Retrieved from https://search.proquest.com/openview/4d23420c8920ed8a70f49cbc421adbf3/1?pq-origsite=gscholar&cbl=26142
13. Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, *57*(5), 1344-1371. Retrieved from https://www.sciencedirect.com/science/article/pii/S1389128613000042
14. Zhang, Xinwen, et al. "Name-based neighbor discovery and multi-hop service discovery in informationcentric networks." U.S. Patent No. 9,515,920. 6 Dec. 2016. Retrieved from https://patents.google.com/patent/US9515920B2/en
15. Calyptix. (2016, March 17). *Top 5 Risks of Cloud Computing*. Retrieved from https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/
16. McLellan, C. (2015, February 2). *Cybersecurity in 2015: What to expect*. Retrieved from https://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/