Information Security

Viselance

Institution

Abstract

Information technology is the use of computers or any other electronic device to store, process, send, or transfer information or data for businesses or personal purposes. Information technology security (IT Security) is the act of implementing systems, policies, and measures that are designed to protect and secure critical information. Homeland security is a term used to describe the department or mission to preserve a state or country from various threats. Therefore, IT Security is essential to Homeland Security because in many cases, technology has presented risks to the public such as cyber-attacks and hackings.

It is identified that the continuous advancement of technology has raised the need for security for the people, businesses, and the government. Many people have been victims to computer crimes and invasion of privacy from time to time. Also, high profile private companies are experiencing tough times of hacking whereby their confidential data is exposed to unauthorized personnel. The government has sensitive data that needs to be kept safe, any alteration or exposure of this information can compromise state security.

Homeland security's IT security sector is focused on national security, public health, and privacy for citizens, safety for businesses, and the economy. The department, therefore, works to ensure that all these areas are protected equally from cyber-attacks. The department of homeland security has so far developed various systems that aim to provide IT Security. Information Technology security is provided for the following purposes: confidentiality, assurance, integrity, availability, and accountability.

This paper will discuss the forms of Information Technology Security systems that have been implemented by homeland security and how they are managed to protect the homeland.

Threats of Information Technology

In contemporary society, every aspect of our lives depends on technology; economic status, health, businesses, government activities, and many more. Any malicious use of information technology can harm many individuals thus the need for security programs that enable protection to the public. Homeland security has worked very hard to ensure these programs are effective. In 2018, homeland security implemented a strategy that would them set up various IT security systems that would reduce the effects of the rising cases of cyber-attacks (DHS Cybersecurity Strategy, 2018). These systems cater for the following: building resistance to attacks, identifying malicious activities, respond to computer attack incidents, and retaining safe and secure technology usage.

According to the Homeland Security department, in the last decade technology has dramatically changed the world. These changes have been positive and negative; technology has enhanced communication, business growth, efficient functioning of multiple government entities. Also, with the advantages, there have been various adverse effects to the community such as increased cybercrimes which have been facilitated by people who want to exploit the vulnerabilities of the cyberspace (DHS Cybersecurity Strategy, 2018). These crimes are motivated by political ambitions, financial gains, infiltration, and other personal ideologies. Criminals are inspired by the curiosities of information technology and with time they are also advancing their attacks thus increasing the threat to the public.

Besides, the introduction of low-cost cyber tools in the technology market has a significant impact on the increased trends of cyber-attacks. For example, Ransomware is a cyber-tool that facilitates attacks on information systems and backup drives. It is identified to have been used in multiple attacks by criminals to bypass traveling, communication, and healthcare systems. Also, sites like the Darkweb are used by people to buy and sell illegal commodities, exchange sensitive data, commit crimes such as terrorism, and many more. The

very existence of Ransomware and Darkweb facilities increases the threats to citizens. Additionally, cryptocurrencies have also been questioned because they foster criminal businesses such as money laundering and cartel businesses.

Managing Information Security

Homeland security has an objective to use innovative strategies with the help of the widely available resources. It has seven key goals to the management approach of Cybersecurity. Firstly, their goal is to identify risks by understanding the evolution of computer crimes so that they can set up risk management strategies. Secondly, to reduce vulnerabilities in government information systems by ensuring all state agencies have high technology security measures. Thirdly, to protect critical infrastructure by collaborating with primary stakeholders to efficiently manage IT security risks (Evans, 2018). Fourthly, to improve response to IT security issues by mitigating effects of potential dangers by encouraging the public effort to respond to these incidents.

In addition, to strengthen technology security and the ability to rely on IT security measures through improving risk management strategies. Lastly, to enhance the management of homeland security IT security systems with techniques that foster consistency. However, all these goals can only be met by understanding the root of IT threats and the effect on national security. This way it will be easier to implement strategic level systems that capture all these areas ("DHS Cybersecurity strategy ", 2018). Besides, the homeland security department focuses on the attempt to improve the challenges of IT security labor force and advising various organizations or institutions to acquire human resources with competent computer security skills and knowledge.

According to Shepardson (2018), the Department of Homeland Security implemented a strategy to deal with the vulnerabilities of the cyberspace threats (3). The strategy is set to

strengthen IT security activities by limiting the activities of malicious actors. Homeland security acknowledged that nation-state cyber criminals are less of a threat compared to non-state criminals who are said to have many advances skills that are hard to deal with under the security measures. Therefore, the goals are to ensure that these sophisticated criminals are cut off of the state's information technology systems.

Evans (2018) explains that homeland security has made Cybersecurity their primary function. The homeland department has an aim to connect about twenty billion devices to the internet that measure the safety of cyber activities by 2020. Therefore, the strategy, policy and plans sector collaborated with the components of the department to come up with effective strategies that address the issue of non-state malicious actors (Evans, 2018). In the end, the department of homeland security wants to shift the advantage from cybercrime actors to people who are trying to improve IT security and their resources play a significant role in this approach.

Furthermore, Homeland security has set up academic programs that educate people about the importance of Cybersecurity. The need for this education program is to improve the understanding and creation of new strategies in response to Information technology threats (Kessler and Ramsay, 2013). This because according to their knowledge, solving security issues requires technical solutions that can only be gained through educational knowledge. The homeland security program, therefore, provides people with information technology security skills based on other topics such as sociology, diplomacy, national defense, and economics. Such technical skills are critical to the Cybersecurity issue.

Preventing cyber/computer crimes

IT security and law enforcement are essential for IT security to secure and protect information systems. For instance, there are special entities that are primarily dedicated to

protecting the *U.S Secret Services* and the *U.S. Immigration and Customs Enforcement* from computer crimes ("Combating Cyber Crime" n.d). This is the most critical components of the United States government that can be highly compromised if attached by malicious cyber attackers. Firstly, the U.S secret service department has *Electronic Crimes Task forces* that duty is to identify and locate cyber criminals involved with bank fraud, data trespass, information system intrusions and many more. This intelligence division has arrested multiple cyber malicious actors.

The Secret Service also manages the *National Computer Forensics Institute (NCFI)*; this institute provides cyber training and cybercrime protection information to all kinds of law enforcement officers. Secondly, the *Immigration and Customs Enforcement, Homeland Security* and *Cyber Crimes Center* offers support services to both local and international investigations("Combating Cyber Crime" n.d).. Also, the department of homeland security has cyber incident reporting resources that provided nationwide details on how and what to report an IT security concern or incident. These entities have significantly reduced the number of computer crimes committed in the state.

Federal systems and Infrastructure protection

Federal corporations use information technology systems for their numerous operations. These types of corporations face cyber threats from state hackers and sophisticated non-state hackers using high computer intrusion techniques. In most cases, such corporations are attacked by people who want to steal or destroy sensitive data. Also, in some situations, an attacker may detain or corrupt the information systems thus denying corporation access ("Securing Federal Networks" n.d). Therefore, homeland security focuses on working with federal corporation departments and agencies to implement policies and measures that reduce vulnerabilities and enhance response to the evolving IT system threats.

These measures are programmed to give alerts whenever a malicious act is detected in the IT systems.

The *National Cybersecurity Protection System* (NCPS) is a division that seeks to improve IT security in state departments, agents, and associated firms by creating technologies that provide security services. These technologies devised by the NCPS can detect system intrusion and prevent intrusion thus reducing the rate of cyber-crimes and threats to federal information ("Securing Federal Network ", n.d). Also, this division improves the responsibilities of homeland security by reducing their workload. The department of homeland security has a program that primarily provides constant monitoring and reduction of information systems, *Continuous Diagnostics Mitigation* (CDM). The CDM program was created for the provision of adequate and cost-efficient Cybersecurity and proper allocation of IT security resources.

Homeland security also has a center for *National Cybersecurity and Communication Integration* (NCCIC) whose mission is to mitigate the risks of information systems and the challenges that may occur. The NCCIC was formed in 2009 to serve as a division for expertise, integration, and communication to Cybersecurity awareness ("Security Federal Network", n.d). It also creates a basis for analysis that hinders malicious activities in federal information systems — besides, the department of homeland security allies with federal agencies to compare and report Cybersecurity issue by the use of metrics for previous and current years.

Moreover, homeland security has employed various resources to protect critical infrastructure that requires privacy. Multiple agencies are asked to provide information and analysis of IT threats and weaknesses to understand the safety of infrastructure. This aspect of gathering information metrics from various agencies help the homeland to determine how

to protect, reduce, acknowledge and recuperate from cyber-attacks ("Protecting Critical Infrastructure", n.d). Therefore, with this information, they can establish a way which they can apply to increase Cybersecurity off the appropriate infrastructure. There are three divisions dedicated to this function namely: NCCIC, *Critical Infrastructure Cyber Community Voluntary Program* (C3VP), and the *National Infrastructure Coordinating Center.*

Cyber Attack Response

Homeland security provides help to affected organizations or entities whenever they are facing IT security issues. They will study the impact of the attack in various infrastructures and investigate to identify the cybercriminal responsible for the attack in collaboration with law enforcement agencies ("Cyber Incident Response", n.d). Besides, the department works with other firms that share the same Cybersecurity mission to ensure that effective response to cyber-attacks.

Conclusion

The Department of Homeland Security is working very hard to ensure that the public is protected from cyber-attacks in various aspects. All the programs set up by the department aim at educating people and creating awareness about the importance of Cybersecurity skills in the country. Computer crimes are a massive threat to national security, and the measures are taken for every division are critical to the mitigation of cyber threats. Therefore, homeland should continue to encourage innovation and establish more education programs for effective response and reduction to information system attacks. It is an era of advanced technology, and the only way to surpass these crimes is to take the technological advantage from cyber criminals by embracing technology.

References

Combating Cyber Crime. (n.d). Retrieved from https://www.dhs.gov/cisa/combating-cyber-crime

Cyber Incident Response. (n.d). Retrieved from https://www.dhs.gov/cisa/cyber-incident-response

DHS Cybersecurity Strategy. (2018). Retrieved from https://www.dhs.gov/publication/dhs-cybersecurity-strategy

Evans, H. (2018). The Department of Homeland Security's Cybersecurity Strategy.*Lawfare.*

Kessler, G. C., & Ramsay, J. (2013).Paradigms for cybersecurity education in a homeland security program.*Journal of Homeland Security Education*, 2, 35.

Protecting Critical Infrastructure. (n.d). Retrieved from https://www.dhs.gov/cisa/protecting-critical-infrastructure

Securing Federal Networks. (n.d). Retrieved from https://www.dhs.gov/cisa/securing-federal-networks

Shepardson, D. (2018). Homeland Security unveils new cyber security strategy amid threats. *Reuters.*