Information Systems Security

Cybersecurity Professionals and Their Tasks

Cybersecurity is a practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.

These are the following tasks of cybersecurity professionals:

- Utilizing every type of medium to stay on top of technology and security threats
- Being aware through analyzing and evaluating threats
- Going through all the systems to check for any potential issue
- Putting proper security measures in place and establishing a protocol
- Creating reports for shareholders
- Spreading the word about security and its importance throughout the company.

Four (4) Cybersecurity Career Paths

1. **Security Architect** – This individual is responsible for maintaining the security of a company's computer system. They must think like a hacker would because they must anticipate all of the moves and tactics hackers will use to try and gain unauthorized access to the computer system. They sometimes have to work odd hours and must constantly stay updated on the latest developments on both the security end and the attacking end. Many information technology experts feel that the best security architects are former hackers since they are adept at understanding how the hackers operate.
2. **Security Consultant** – S/He works as an advisor and supervisor for all security measures necessary to protect a company or client's assets effectively. S/He uses his/her knowledge and expertise to assess possible security threats and breaches for prevention and create contingency protocols and plans for when violations occur.
3. **Ethical Hacker** – Also referred to as a white hat hacker, s/he is an information security expert who systematically attempts to penetrate a computer system, network, application, or other computing resources on behalf of its owners, and with their permission, to find security vulnerabilities that a malicious hacker could potentially exploit.
4. **Chief Information Security Officer (CISO)** – This person is responsible for an organization's information and data security. The CISO's job is to learn what day-to-day responsibilities will fall under its umbrella. Examples are security operations, data loss, program management, and access management.

Introduction to Risks, Threats, and Vulnerabilities

THE ANATOMY OF CYBERATTACK

Step 1: Reconnaissance

Hackers usually start by researching and gathering information about the target organization. They look for network ranges, IP addresses, and domain names. They also search for e-mail addresses of key players in the organization, such as IT professionals.

If the hackers fail to find the e-mail addresses of the key players, they identify vulnerable employees by sending phishing e-mails. Then, the attackers scan for vulnerabilities in the network, which is a long process that sometimes take months. After they get an entry to the organization via network vulnerabilities or employee e-mail address, the attackers proceed to the next phase.

Step 2: Attack
After getting access to the network, hackers proceed with infiltrating the organization's network. But to access the network freely, they need access privileges. Hence, attackers use rainbow tables and similar tools which help them with stealing credentials to upgrade their access to administrator privileges.

Now, hackers can access the entire network and go through the networks silently. Then, attackers are free to obtain sensitive information for selling on the Internet or encrypt the data to demand a ransom. Sometimes, hackers alter or erase sensitive data for reasons beyond financial gain.

Step 3: Expansion
Hackers intrude all systems on the network using malicious programs. Malicious programs enable attackers to hide in multiple systems in the organizations and regain access to the network even after being detected. Additionally, hackers no longer require higher access to infiltrate the network.

Step 4: Obfuscation
Hackers proceed to hiding their tracks to mask the origins of the attack. Additionally, they safely place their exploit in a system to avoid getting detected. The main purpose of obfuscation is confusing and disorienting the forensic experts. For successful obfuscation, hackers use various tools and techniques such as spoofing, log cleaning, zombie accounts, and Trojan commands. Cybersecurity experts generally consider obfuscation as the final stage of the anatomy of a cyber attack.

Seven (7) cybersecurity risks that may impact organizations

1. **Technology** – While technology has revolutionized the way organizations conduct business today, the broader and widespread use of technology also brings vulnerabilities. From publishing to automotive, industries are facing new, evolving services and business models. These new opportunities, however, bring with them a radically different set of risks, which organizations will need to anticipate and manage as they continue the digital transformation process.
2. **Supply Chain** – Two (2) prevailing supply chain trends will heighten cyber risks dramatically in the coming year: one (1) is the rapid expansion of operational data exposed to cyber adversaries, from mobile and edge devices like the Internet of Things (IoT); and the other trend is the companies' growing reliance on third-party and even fourth-party vendors and service providers. Both trends present attackers with new openings into supply chains and require board-level, forward-looking risk management to sustain reliable board-level and forward-looking risk.
3. **Internet of Things (IoT)** – IoT devices are everywhere, and every device in a workplace now presents a potential security risk. Many companies don't securely manage or even inventory all IoT devices that touch their business; these already result in breaches. As time goes by, the number of IoT endpoints will increase dramatically, facilitated by the current worldwide rollouts of cellular IoT and forthcoming transition to 5G. Effective organizational inventory and monitoring process implementation will be critical for companies in the future.
4. **Business Operations** – Connectivity to the Internet improves operational tasks dramatically, but increased connectivity also leads to new security vulnerabilities. The attack surface greatly expands as connectivity increases, making it easier for attackers to move laterally across an entire network. Further, operational shortcuts or ineffective backup processes can make the impact of an attack on business operations even more significant. Organizations need to be better aware of and prepared for the cyber impact of increased connectivity.
5. **Employees** – Employees remain one of the most common causes of breaches, yet they do not even realize the true threat they pose to an entire organization's cybersecurity. As technology continues to impact every job function, from the CEO to the entry-level intern, it is imperative for organizations to

establish a comprehensive approach to mitigate insider risks, including strong data governance, communicating cybersecurity policies throughout the organization, and implementing effective access and data-protection controls.

6. **Regulatory** – Increased regulation, laws, rules, and standards related to cyber are designed to protect and insulate businesses and their customers. Regulation and compliance, however, cannot become the sole focus. Firms must balance both new regulations and evolving cyber threats, which will require vigilance on all sides.
7. **Board of Directors** – Cybersecurity oversight continues to be a point of emphasis for board directors and officers, but recent history has seen an expanding personal risk raising the stakes. Boards must continue to expand their focus and set a strong tone across the company, not only for actions taken after a cyber-incident but also for proactive preparation and planning.

Cybersecurity Threats and Vulnerabilities

- **Ransomware** is a type of malicious software designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom, however, does not guarantee that the files of the system will be recovered or restored.
- **Malware** is a type of software designed to gain unauthorized access or cause damage to a computer.
- **Social engineering** is a tactic that adversaries use to trick a user into revealing sensitive information. They can solicit a monetary payment or gain access to confidential data. Social engineering can be combined with any of the threats to make the user click on links, download malware, or trust a malicious source.
- **Phishing** is the practice of sending fraudulent e-mails that resemble e-mails from reputable sources. It aims to steal sensitive data like credit card numbers and login information. It is the most common type of cyberattack.
- **Crypting services** are used for encrypting malware to obscure and make the data difficult to detect.
- **Crimeware** is the buying and selling of malware on the "Dark Web," a black market for cyber criminals. It is a software designed to enable other people (typically those with minimal technical skills) to become cyber criminals.
- **Remote administration tools** are a type of malware that, once activated, grants hackers control over the infected computer. The attacker can then proceed with stealing data from the machine, rendering it inoperable, and using the camera.
- **Keyloggers** are malware that tracks keystrokes, enabling the attacker to eavesdrop on confidential conversations and steal login credentials.
- **Exploit kits** work by targeting users who think they are visiting a trusted site but then get redirected to a malicious site.
- **Leaked data** are data stolen from a user's machine that can easily be sold on the Dark Web. Examples include credit card numbers, social security numbers, and corporate login credentials.
- **Card skimmers** are implanted in places like Point-of-Sale (POS) machines, bank teller machines, and gas pumps to steal identity and credit card account data.
- **Unpatched systems** – A great proportion of cybersecurity vulnerabilities can be resolved through the application of software patches. However, for reasons related to IT operations, and in some cases to aging software, a lot of systems may lack security patches. These outdated systems are vulnerable to attack.

The CIA Triad

Confidentiality ensures that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess them. It is implemented using security mechanisms such as usernames,

passwords, access control lists (ACLs), and encryption. It is also common for information to be categorized according to the extent of damage that could be done should it fall into unintended hands. Security measures can then be implemented accordingly.

Integrity ensures that the information is in a format that is true and correct to its original purposes. The receiver of the information must have the information the creator intended him/her to have. Only the authorized persons can edit the information. It will remain in its original state when at rest. Integrity is implemented using security mechanisms such as data encryption and hashing. Note that the changes in data might also occur as a result of non-human-caused events, such as electromagnetic pulse (EMP) or server crash. It is important to have the backup procedure and redundant systems in place to ensure data integrity.

Availability ensures that information and resources are available to those who need them. It is implemented using methods such as hardware maintenance, software patching, and network optimization. Processes such as redundancy, failover, RAID, and high-availability clusters are used to mitigate serious consequences when hardware issues do occur. Dedicated hardware devices can be used to guard against downtime and unreachable data due to malicious actions like distributed denial-of-service (DDoS) attacks.

Data Classification Standards

This standard aims to establish a framework for classifying data based on its level of sensitivity, value, and criticalness. Classification of data will aid in determining baseline security controls for the protection of data.

- **Understanding** – The cycle of managing data begins with understanding what the data is, how it has been classified, and where it will be located. The information management life cycle is iterative and will keep looping back in understanding data. For example, as data changes and becomes aggregated, it may need to be reclassified.
- **Creating** – This includes, but is not limited to, collecting data, experimenting, observing, and measuring and simulation.
- **Storing** – This includes, but is not limited to, designing research, locating existing data, and capturing and creating metadata.
- **Using** – This includes, but is not limited to, entering data, digitizing, transcribing and translating, checking, validating, filtering and cleaning data, anonymizing data where necessary, describing, managing, interpreting, and deriving data, and statistical analysis.
- **Sharing** – This includes, but is not limited to, distributing, sharing, promoting data, controlling access, establishing copyright, producing research outputs and author publications, preparing data for preservation, and using the data classification definitions to help the user through this process.
- **Archiving** – This includes, but is not limited to, migrating data to the best format and suitable medium, backing up and storing data, creating metadata and documentation, and archiving data.
- **Destroying** – This includes, but is not limited to, disposing of data, destroying paper records and electronic media, and electronic shredding.

References:

Bashay, F. (2018, February 2). What is the CIA triangle and why is it important for cybersecurity management? [Web log post]. Retrieved from https://www.difenda.com/blog/what-is-the-cia-triangle-and-why-is-it-important-for-cybersecurity-management on April 22, 2019

Destroying (n.d.). In *Information Security*. Retrieved from https://security.uwo.ca/information_governance/standards/data_handling_standards/destroying.html

Ethical hacker (n.d.). In *TechTarget*. Retrieved from https://searchsecurity.techtarget.com/definition/ethical-hacker on April 22, 2019

Fruhlinger, J. (2019, January 4). What is a CISO? Responsibilities and requirements for this vital leadership role [Web log post]. Retrieved from https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html on April 22, 2019

Goolik, S. (2019, March 19). 2019's cyber security vulnerabilities & best practices to protect your business [Web log post]. Retrieved from https://symmetrycorp.com/blog/8-cyber-security-vulnerabilities/ on April 22, 2019

Joshi, N. (2018, December 22). The anatomy of a cyberattack: dissecting the science behind virtual crime [Web log post]. Retrieved from https://www.allerin.com/blog/the-anatomy-of-a-cyber-attack-dissecting-the-science-behind-virtual-crime on April 22, 2019

New Horizons Computer Learning Centers (2018, July 19). 4 cybersecurity career paths (And the training to get you there) [Web log post]. Retrieved from https://www.newhorizons.com/article/4-cybersecurity-career-paths-and-the-training-to-get-you-there on April 22, 2019

Security architect. (n.d.). Retrieved from https://www.infosecinstitute.com/career-profiles/security-architect/ on April 22, 2019

What does a security consultant do? (n.d.). In *Neuvoo*. Retrieved from https://neuvoo.ca/neuvooPedia/en/security-consultant/ on April 24, 2019

What is cybersecurity? (n.d.). In *Cisco*. Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html on April 22, 2019

What is a cyber security professional (n.d.). In *Career School Now*. Retrieved from https://careerschoolnow.org/careers/cyber-security on April 22, 2019