Overview of the Importance of Corporate Security in business

Sourav Mukherjee

Senior Database Administrator &

PhD student at University of the Cumberlands

Chicago, United States

Abstract

This article gives an overview of the importance of corporate security in today's business. Information security has stood out as paramount importance to organizations. The security of any system and people continues to remain a top priority for the company. In every organization or business, the employees can possibly represent their organizations to enormous amounts of cyber risks. Every employee in the organization have accountability to remain vigilant and properly respond to security threats as they arise. In today's busy World, every corporate security is focusing on ensuring that they secure their customers, facilities, systems and ensure that they are designing security into their client solutions. Few key initiatives include collaborating with the IT organization on foundational projects such as securing remote access, transforming the identity and access administration services and improving the identification and remediation of vulnerabilities. As we seek to protect the company's brand name and the client's trust, it is vitally important for every organization to consider security a key responsibility. When organizations choose to disrespect security policies & procedures, the organization is at danger. Through the organizational control lens, tried to explain the corporate security precaution-taking behavior. In this article, we will discuss how the security attack happens and how can it be prevented, data security and cybersecurity.

Keywords: Data, Security, Cybersecurity, Attack, Phishing, Malware, Risk, Ransomware, Information Security.

Introduction

Why is security being vital in all organization suddenly? A couple of years back, mostly engineers used to worry about cybersecurity. Now a day, commercial leaders in every company extensively observed the need for strong security in their IT divisions. Previously if antivirus, encryption tools, accurate firewalls are in place, leadership used to leave the responsivity on their experts and try to an emphasis on other critical things on the business. Though security was a vital point every company thinks, in the past leadership used to think that expert can deal with the security of data leaking, protection, data reduction, etc. Everyone's focus is to secure the data especially when it comes to the Banking sector, Insurance and deals with customer's money. Data is the most important asset in any organization. As dealing with customer's data is not so easy, every company is coming up with a different strategy to handle the sensitive customer's data, handling the phishing attacks, strong password management, creating awareness for everyone working in the company and how to overcome with cyber-attack when happens. Data leakage can cause a huge loss in the organization, so every organization thinks about data privacy at the first point to protect their sensitive data. Not following the guidelines of data protection may cause loss or theft of company intellectual property, damage to the organization's reputation, corporate or individual penalties and compromising the system to hacking or malware infection vulnerabilities.

Literature Review or Background

So, what's changed that cybersecurity became an important factor to discuss in every organization? Cybersecurity or information technology security is the methods of caring processers, networks, programs and data from illegitimate, unlawful, illegal access or occurrences that are intended for exploitation or corruption. Network safety contains doing things to protect the usability, dependability, veracity, and protection of the network. The unlawful photocopying of the data is a violation of any company. It may cause loss or theft of the company's intellectual property and damage the company reputation. So, every company needs to follow some security practices to reduce the risks and mitigate threads. A fruitful and effective cybersecurity method has several layers of protection feast diagonally the networks, computers, programs, or data that one proposes to keep safe. The technology, people and the processes in an organization collaborate with each other to produce operative protection from cyber-attacks.

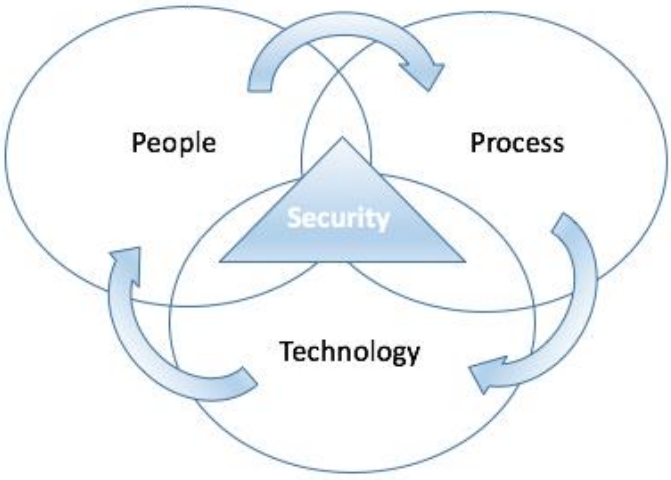

Fig1: The People, Processes, and Technology triad for information security

Technology: Technology is a vital factor to consider for cybersecurity in any organization - the security tools that desire to protect the network from cyber-attacks. The endpoint devices such as computers, smart devices, routers, networks, and the cloud are essential to be protected using a firewall, malware software protection, antivirus, DNS filtering, email phishing solutions.

People: People or employees need to understand the critical issues about cyber-attack and to protect that they can use strong password, not to open any suspicious attachment in email, always zip the files or document while sending via email, saving system or any other password in secure places, not to open any site which looks suspicious. Also, no one should leave any devices like laptop, computer unattended, always must be very careful while opening any attachment in the email, browsing any site from secure Wi-Fi or internet, take the data back up regularly, etc. are most important cybersecurity tips for users.

Processes: Every organization has some processes set up how to deal with the cyber-attack. An essential supporting structure will help how the cyber-attack can be recognized, how to protect the network and systems, perceive and reply to intimidations, and recuperate from fruitful attacks. Cybersecurity task best practices can be outlined to overcome the threats which will contain specific information on security controls (whitelisting IP addresses, firewall access, etc.). Vulnerability scanning boxes can be set up with the latest released software to scan on each system periodically and keep eye on the traffic.

Importance of security:

Today all the programs and functions are associated, all organizations want to take assistance when it comes to the security. Data leakage can cause a huge loss at an individual level also at the organization level, so every individual and organization think about data privacy at the first point to protect their sensitive data. At individual level data loss can happen from the mobile phone, email, social media, browsing any untrusted sites whereas in organization level it will be a huge loss as they deal with customer's data. Where the individual can stop browsing any untrusted site, an organization can follow the below for data protection.

- Implement data encryption/hashing on the device and server.
- Sensitive local data stored encrypted with user secret that encrypts the data encryption key.
- Use NIST (National Institute of Standards and Technology) approved encryption standard algorithms to encrypt the sensitive data.
- Encryption keys shall never be in RAM. Instead, keys should be generated real-time for encryption/decryption as needed and discarded each time.
- No sensitive data (e.g. passwords, keys, etc.) in cache or logs.
- Use remote wipe APIs.

- Do not reveal UDID (unique device identifier), MSISDN (Mobile Station International Subscriber Directory Number), IMEI (International Mobile Equipment Identity) and PII (Personally Identifiable Information).

Types of security and recommendation to overcome it:

Physical Security

The following recommendations are important controls to physically secure the application within the environment:

- Physically locate servers in an access-controlled environment.
- Protect physical access to server and network equipment locations with locking devices.
- Provision devices with redundant power supplies.
- Disable unused physical ports on network equipment.

Network Security

The following recommendations are important controls to secure network communications of an application within your environment:

- Employ network segregation (VLAN, router, firewall) and create a secure enclave to protect the application.
- Prevent any in-bound Internet communications to the application from external locations.
- Configure network level authentication to control and limit device connectivity

- Ensure remote access sessions transmit via a secure protocol (VPN / IPSEC, SSH tunnel).
- Use strong wireless protocols.
- Employ intrusion detection mechanisms to monitor for unauthorized network access.

Operational Security

The following recommendations are important controls to secure the operational integrity of an application within the environment:

- Maintain all clients and servers with up-to-date security patches.
- Deploy and maintain anti-malware software on all clients and servers.
- Restrict local operating system and database administrative access to the maximum extent possible.
- Define privileged accounts according to need-to-know access, least privilege, and segregation of duties.
- Enforce strong application password policy by integrating the application with enterprise LDAP directory services.
- Ensure database backups occur daily and are protected by physical security or encryption when they are stored.
- Ensure data exports by application clients use encrypted portable media only.
- Configure audit logging on all servers and consider integration with a centralized security event monitoring system.

- Deploy software to monitor and alert when critical system resources (disk, memory, CPU) are low.

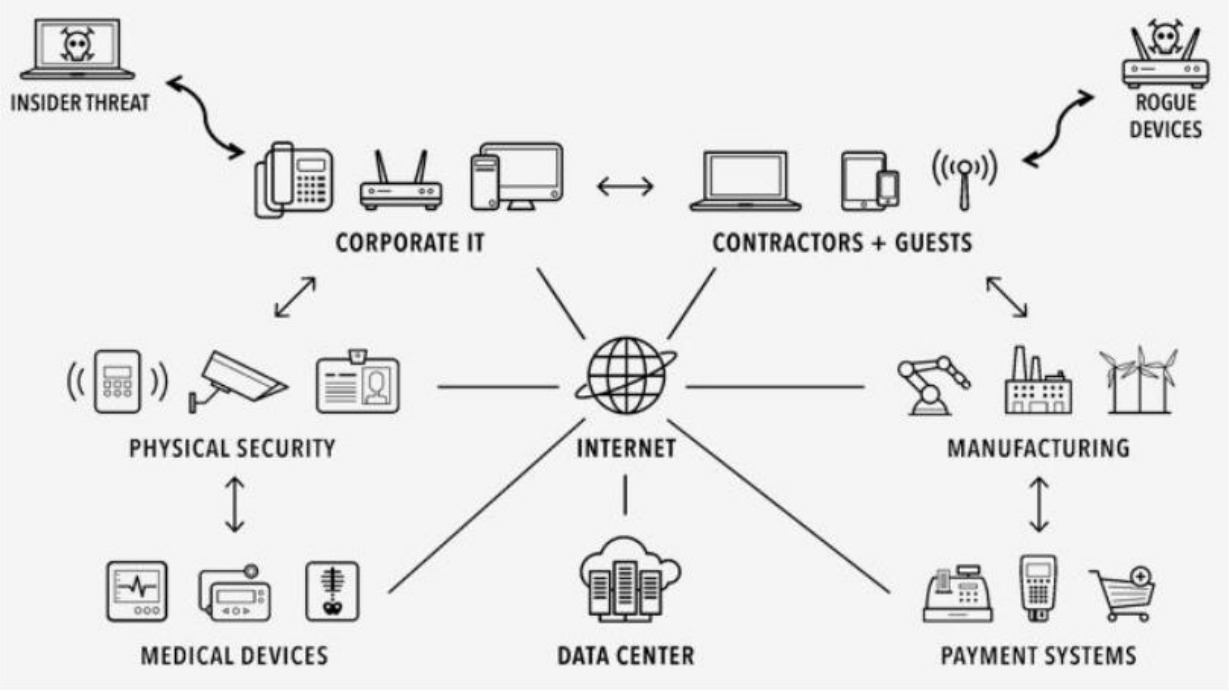

Fig2: The overall diagram shows the security and threat

Corporate Security Highlights:

Ransomware: It is a type of malicious software intended to transfer currency by blocking access to records or the computer system until the payment is done. Once the payment is done that is not guaranteed whether the records are recovered. To get rid ransomware a good antivirus utility can run frequently and keep the browser related components updated. Do not open any attachment from any unexpected email or do not download anything from the spam folder. Always keep your back-up updated so if anything happened you can re-install everything freshly.

Malware: Malware is also a malicious software which is intended to have illegal access to harm a system. One approach for protecting in contradiction of malware is to stop the malware software from obtaining access to the target computer. An antivirus software, firewalls, and other approaches can be used to help to protect a malware function, in that, in addition, inspect for the availability of malware and malicious activity and recovering from attacks.

Phishing: Phishing is an exercise of transferring fake emails that look like normal emails from trustworthy sources. The purpose is to get information about all sensitive data like login details, password, debit/credit card numbers, etc. which is very well known cyber-attack practices. There can be different types of phishing like spear phishing, whaling, pharming, etc.

Spear phishing is when the attacker target individual instead of targeting the group of people. Attacker search for their social media sites to get information about the person. That way they can show how authentic they are. For example, when you do online shopping, they will send an email with a link asking for feedback which will look so authentic. Once you click the link, the set of questions will be there to answer which is fraudulent. This can be avoided by filtering nasty emails and not opening them.

Whaling is when assailants go behind a big-fish like CEO of the company. The assailants frequently spend significant time outlining the target to discover the appropriate instant and means of stealing login identifications. Whaling is of apprehension because high-level officials can access an unlimited contract of business information.

Pharming is like phishing which sends users to a fake website that seems to be genuine. However, in this case, users do not click a link to be taken to the malicious site. Attackers can infect either the user's computer or the website's DNS server and redirect the user to a fake site even if the correct URL is typed in.

Not following the security guidelines can lead to:

- Loss or theft of company intellectual property.
- Damage to the organization's reputation.
- Corporate/Individual penalties.
- Compromising the system to hacking or malware infection vulnerabilities.

Crisis Management:

What is a Crisis?

A Crisis is defined as a major incident that positions substantial risk to the security and safety of personnel, facilities, achievement of its processes, and the truthfulness of its status. The best practices should be whenever an associate becomes aware of a situation that has the potential of escalating to a crisis, the individual must notify corporate security immediately. There must be some hotline numbers or email groups where an incident can be reported, an employee must be trained about the processes.

A corporate framework can be created to help provide a structured and predetermined response to crisis situations. All team members and senior leaders are trained to work together to quickly and efficiently respond to crisis events, coordinate support and assistance, and help limit the overall impact on corporate business.

Key objectives of the corporate framework will include:

- Establishing sound crisis management and preparedness through training and ongoing monitoring of world events.
- Maintaining plans and teams who can respond quickly, to minimize a crisis' impact on corporate business.
- Managing effective upstream and downstream communications in the event of a crisis.
- Having up-to-date information, contacts, emails of all employees in one system which allows the crisis management team to deliver time-sensitive information such as critical alerts, information on safe locations, emergency contacts, and ongoing incident updates.

How an individual can help the organization for security?

- Confidential customer's information from corporate id to personal email accounts should not be sent.
- Never copy customer's data to online personal storage or to personal storage devices

- Never click on links or open attachments in suspicious emails.
- Never leave confidential, sensitive, Personally Identifiable Information and Protected Health Information in your workplace in an unsecured manner
- Report all security incidents immediately to the corporate security team.

Password Security Best Practices

Strong and secure passwords are the first line of defense against computer hackers. If a password is exposed, confidential data stored on various systems, applications, and networks may be at risk. Below are some password best practices:

The password is very confidential and should not be shared with anyone.

- Always select a complex and strong password that is hard to crack and adheres to corporate password standards.
- Never write passwords down anywhere where it is easily accessible to others.
- Report any password sharing incidents to the corporate security team in the organization.

Conclusions and Future Study

To conclude investment in computer-based security-related training, awareness and mentoring program may eventually protect the organization as individuals with skilled proficiency in computer better understand what they need to do to in order to protect corporate computer assets and can create a security-conscious culture. Human error is one of the key reasons in which systems are breached. However, if the corporate team are educated and have a good sense of

understanding of risks and the potential significances, it may stand to be the first line of defense in a multi-faceted tactic to preserving the overall corporate security.

These findings reveal a lot of insights into how to form the security controls and its implications of management actions in offering a secure corporate environment. While the individual is standing at the borderline of defense in information security, it is imperative that organizations should offer strong expertise in computer policies & procedures and perform all they can do to inspire individuals to comply. This study reveals that the ways of implementing corporate information security policies which goes beyond making the policy and dictates the individuals in the organization that the policies are extremely obligatory. More intensive care is needed in order to accept the policies at the management level to offer such policies backed by real-life training and assessment in order to motivate employees to advocate a more secure computing environment.

As security is the top priority for the company, every organization should have a corporate security team who can work better align to risk management activities to the security risk profiles of the customers. Periodically a survey can be conducted and using survey data, the security team in the organization will examine the services provided, the corresponding potential data exposure, and the associated contract liability to determine the level of oversight that company will provide to individual customers. The objective of this exercise is to ensure the highest and best use of security to reduce information security risk.

References

[1] Author Jimmy Spencer, July 6, 2018, retrieve from https://securityfirstcorp.com/why-is-cyber-security-important/

[2] Cisco, retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[3] Cisco, retrieved from https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

[4] Mukherjee, S. (2019). Popular SQL Server Database Encryption Choices. arXiv preprint arXiv:1901.03179.

[5] Mukherjee, S. (2019). Benefits of AWS in Modern Cloud. arXiv preprint arXiv:1903.03219.

[6] Mukherjee, S. (2019). How IT allows E-Participation in Policy-Making Process. arXiv preprint arXiv:1903.00831.

[7] Mukherjee, S. (2019). Popular SQL Server Database Encryption Choices. arXiv preprint arXiv:1901.03179.

[8] Chakraborty, Moonmoon & Excellence, Operations. (2019). Supply Chain & Inventory Management. 10.6084/m9.figshare.7824107.

[9] Fig1: Author Tony Perez, OCTOBER 31, 2015, retrieve from https://perezbox.com/2015/10/website-security-is-not-an-absolute/

[10] Fig2: Author Susan Ranford, Mar 29, 2018, retrieve from https://www.ittropolis.com/physical-security-just-important-online-security/

[11] Mukherjee, S. (2019). Indexes in Microsoft SQL Server. *arXiv preprint arXiv:1903.08334*.

[12] Chakraborty, Moonmoon & Excellence, Operations. (2019). Supply Chain & Inventory Management. 10.6084/m9.figshare.7824107.

[13] Chakraborty, Moonmoon & Excellence, Operations. (2019). Supply Chain & Inventory Management. 10.6084/m9.figshare.7824107.

[14] Chakraborty, Moonmoon. (2019). Planning, Control Systems and Lean Operations in Information Technology. 10.6084/m9.figshare.7886138.

[15] Chakraborty, Moonmoon. (2019). Fog Computing Vs. Cloud Computing. 10.6084/m9.figshare.7886126.

[16] Chakraborty, Moonmoon. (2019). Managing Risk, Recovery & Project Management. 10.6084/m9.figshare.7886141.

[17] Mukherjee, Sourav. (2019). How stakeholder engagement affects IT projects. 10.6084/m9.figshare.7886162.

AUTHOR'S PROFILE

Sourav Mukherjee is a Senior Database Administrator and Data Architect based out of Chicago. He has more than 12 years of experience working with Microsoft SQL Server Database Platform. His work focusses in Microsoft SQL Server started with SQL Server 2000. Being a consultant architect, he has worked with different Chicago based clients. He has helped many companies in designing and maintaining their high availability solutions, developing and designing appropriate security models and providing query tuning guidelines to improve the overall SQL Server health, performance and simplifying the automation needs. He is passionate about SQL Server Database and the related community and contributing to articles in different SQL Server Public sites and Forums helping the community members. He holds a bachelor's degree in Computer Science & Engineering followed by a master’s degree in Project Management. Currently pursuing Ph.D. In Information Technology from the University of the Cumberlands. His areas of research interest include RDBMS, distributed database, Cloud Security, AI and Machine Learning. He is an MCT (Microsoft Certified Trainer) since 2017 and holds other premier certifications such as MCP, MCTS, MCDBA, MCITP, TOGAF, Prince2, Certified Scrum Master and ITIL.