ENPM686 - Final Paper

Faraaz Hasan Khan (116794244)
Aayushi Dubey (116934596)

This document (18 pages) contains the Final Paper for ENPM686 - Information Assurance.

S.No	Topic	Page
1	Scenario	2
2	Objective	2
3	Assets To Be Protected	3
4	Threats To The Company	5
5	Weaknesses in the Current System	10
6	Solutions To Threats	13
7	Cost and Budget Plan	16
8	Summary	17
9	References	18

Scenario

A company which takes work from the government on a contractual basis is struggling in terms of security. They recently found malicious activity in their system through their logging system in which many login attempts were made and the admin was compromised, credentials had to go through a reset but logs still show of malicious activity and it may lead to a large scale security failure in the future. The company in this scenario is a small sized firm which takes contracts from the government.

Confidential files are stored in their desktops which are only for company use and cannot be taken out of the premises.The office has 20 computers running windows and currently has 1 security engineer and 11 other employees apart from the CEO, which makes it a total of 13 people (only 1 for security). The company makes ~ $2 million dollars in revenue per year and the CEO wants to allocate 8-10% of that to the complete security architecture of the company.

The contractor does rely on Amazon Web Services as a cloud platform along with desktops to store files.There are a select few security cameras installed on the premises and have a security guard monitoring the entrance.

Since the company deals with government contracts and sensitive information, they cannot afford to lose confidentiality over the data or the data itself. Because of this, the company is willing to spend more money on security by adding more security measures along with security personnel, if required.

Objectives

1. The objective of the paper can be divided into five parts:
2. Determining all the assets that the company owns and uses along with prioritizing each asset with respect to security.
3. Determining the kinds of security threats that could hard company property, personnel and data.
4. Taking a look at the current system and determining the assets that are most vulnerable to threats and assets that are most important and the company cannot afford to put them in harm’s way.
5. Proposing a plan to counter and fill gaps in the current security architecture by introducing new practices and/ or eliminating some existing practices.
6. Alternatives to some components in the events that the cost plan doesn’t allow us to go through with our primary solutions and if we can afford to compromise on our main solution.
7. Estimating the cost plan for the modified security architecture.

Assets To Be Protected

The company wants to protect desktops. In this context, threat actors would want access to those government files and the government contractor isn’t as technologically equipped so It makes the firm a relatively easy target. As mentioned in the scenario, the primary source of information in the firm is desktop computers with cloud and storage services also playing a role in housing data. When we look at desktops, we can say that there is a lot of physical threat to it as well such as the desktop being broken intentionally or unintentionally. Data on these desktops can be accessed by employees in the company if they have access to passwords for the same, which is unlikely but the fact that security engineers or admin knows passwords is likely and if they decide to go rogue, it is possible that the data might be tampered with in some way.

Two kinds of files need security, one is the firm's own files which houses employee details and other company related files and the second being the work that they do for the government. It is important to differentiate the two resources and manage them separately. This will be useful in not just securing data but also managing data efficiently. Moreover, different data needs different models of security and hence, it would be useful on separating the two types of data and if possible, delegate them to two different people and if it isn't possible, then at least the concerned employee should take some measures to divide the two.

There is data on the cloud service as well. The company also has a physical storage policy (hard drives, etc.) along with storing data on cloud and other geographical locations. When we talk about physical storage mediums like USB and hard drives, it gets a lot harder to implement physical security measures. While it is not recommended to use these drives in a company environment as it could easily be stolen temporarily or permanently due its portability and these do not have enough storage on them as well except the drives that could hold upwards of 2 Terabytes of data. Another problem with this company asset is that these do not have enough encryption measures and if it falls into the hands of a potential threat actor, the data could be copied in a matter of minutes. It is possible to buy hard drives which have encryption softwares in them and there is a password required to break if it is connected to an unknown computer but the question is whether the firm is willing to spend hundred plus dollars on a hard drive.

There is also an element of internal threat in which an employee might steal some of the company's files if they get a good offer from threat actors and if they want to participate in such an activity. The problem in this scenario could be that the employees aren't paid a hefty amount of money and they could get greedy if an outsider threat converts an employee into an insider threat for good money. The problem isn't limited to the employees not being paid a lot of money as we've seen in the past that employees earning millions could also turn to insider threats for more. We'll discuss how internal employees could be potential threats later in this paper, but it is a considerable and almost unavoidable problem as you do not know the intentions of an employee while hiring them or their intentions while working for a company as these intentions aren't guaranteed to be traced by a background check.

Taking previously mentioned points into consideration, we can say that when data is tampered with, it leads to disruption of confidentiality, integrity and availability of data, also known as the CIA triad. There are other facets of security like authentication, authorization and non-repudiation that could also be affected.

Threats To The Company

Phishing: - It is one of the most common social engineering techniques used to deceive users. Risk actors try to gain access to the accounts and networks as the company deals with the government, and they contain sensitive information. By means of social media sites or emails, they try to make it look real so that an employee of a company gets convinced to click on the link and consequently, enable a drive-by download or a regular download which install malicious content on their system and hence, the hackers can get sensitive information about through accounts, networks.

Malware: - Malware is several programs or files that are dangerous to a system operator. It includes system trojan, viruses, horses, worms, spyware, and ransomware. These malicious programs can execute a variety of altered functions such as stealing the user's information, encrypting sensitive files and information or deleting sensitive information from the client or server's side, altering the traffic route of sensitive packets or hijacking core computing functions of various servers and monitoring user's system activity without having any kind of permission. Hackers use a different type of substantial and virtual techniques to disperse malware that contaminates programs, networks, and systems. This malicious software can be distributed to a system through physical media like external hard drives or thumb drives, or through the internet by means of wireless connections like Wi-Fi, which generally unconsciously copies malicious software to systems without the user's permission or having any kind of knowledge. The phishing attack is a well-known malware delivery technique where emails masked as genuine emails comprise harmful HTML links or add-ons that can dispense the malware to unsuspicious users. Once the phishing is effective, there are probabilities that dangerous programs are copied in the user's system. A trojan virus is an example of malware brought onto the network as software. Malware is available in different forms and can-do various tasks like spying on the user's system or changing the original codes.

Examples of different malware are: -

Virus: It is the most usual kind of malware that can accomplish itself and disperse by affecting other programs and files.

Worm: This is a self-replicating malware with or without a hosting program and can affect the programs and the files without any human interaction or execution.

Trojan Horse: It is programmed to look like genuine software with the intention of gaining entrance to a system. Once initiated after installation, it can execute their dangerous and infectious tasks.

Spyware: This malware is designed to accumulate information and information like security passwords or card details on the user's device and watch their action exclusive of their awareness.

Ransomware: Ransomware is programmed to corrupt a user's system and encode the information. Cybercriminals then ask for a payment from the victim for their original information, and they have to pay for that information because generally sensitive information and information are targeted.

Rootkit: A rootkit is designed to gain admin access to a system. When it gets installed on a system, then the hacker gains access to all root files on the system and can modify as well as delete important information or steal files; in other words, the hacker then has a backdoor to the system and can do whatever he wants.

Adware: It is designed to keep a record of a person's browser history so that they can display pop-up or banner advertisements related to those browsing history that bait the person into buying those products.

Keylogger: Keyloggers are used to monitor a system and are used to keep a watch on all the activities a user does on their system. This includes financial transactions, emails, webpages, and keystrokes.

Distributed Denial of Services: It is a malicious try to interrupt the regular traffic of a destined server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. DDoS attacks accomplish success by exploiting various compromised systems as the origin of the attack. A compromised system can contain physical systems and networked devices. The DDoS outbreak is like traffic congestion blocking up with highways, avoiding fixed traffic from incoming at its preferred destination. This attack floods the server with requests from multiple sources, which can slow down the server or even crash. Once this is done, the system becomes impossible to use effectively until these attacks are canceled or blocked. A DDoS attack includes a hacker to advance the power of a network of systems so as to convey out the attack. Systems are infected with malware rotating each one into a bot. The person then has remote control over the clutch of bots called a botnet. When a botnet has been started, the person is able to through the machines by transferring revised commands to every bot through a technique of distant mechanism. When the IP address of a target is pointed by the botnet, then each bot will reply by directing demands to the objective server or network to excess volume, resulting in a DDoS to normal traffic. Since every bot is a genuine internet means, splitting the assault traffic from usual traffic can be problematic.

Brute force or password attacks: In this hacker yields a lot of security passwords with the confidence of ultimately predicting accurately. The hacker confirms every potential security password until the right one is located. Otherwise, the hacker can try to predict the key, which can normally be generated after the password by means of a key derivation function. Hackers can try to gain access to a network by means of a package to determine an effective password. A brute force attack can be used to try to decode any encoded information. This type of attack force is used when it is not likely to yield the benefit of further flaws in an encryption scheme that would create the task simpler. This technique is very constant when deployed to order all short security passwords, but for lengthier security passwords, different techniques such as the vocabulary attack are used since a brute-force examination takes too long. Longer security passwords and keys have more possible values, making them exponentially more problematic to decrypt than the passwords that are shorter in length. These attacks can be made less effective by obfuscating the information to be encoded, making it more problematic for a hacker to recognize when the code has been cracked or by making the hacker do more work to test each predict. One of the measures of the strength of an encryption system is how long it would theoretically take a hacker to mount a successful brute-force attack against it.

Ransomware: Hackers gain access to a target network through social engineering like phishing mail. Educating employees on being aware of phishing scam can reduce the risk to the organization by preventing successful breaches before they occur. Once a malicious link is clicked or an infected file opened or even downloaded, the virus is able to gain a grip, quickly infiltrating the network and locking up files. The following phase includes the ransomware virus directing files and also folders. This is the reason due to which the user is prevented from being able to corrupt backup files, making this malware profitable. Victims of this malware often have no choice but to pay the fee or risk losing all of their information with no way to replace or restore it. This is one of the malware that when opened locks the system down and locks the device in such a way that no one can use it again. It is the most damaging malware risk. The device will remain locked until a ransom is paid on its behalf. Once the backups are successfully removed, the ransomware then executes a secure key exchange with the server and puts encryption keys in place. Through the person's substitute documents departed and the encryption effectively-recognized, the ultimate stage includes a report to the person and demand for the planned payment.

Information leakage: Information can be leaked from the particular mobile or system/laptop, so we must ensure that they all contain passcodes, which cannot be easily predicted. Data leak is the unapproved diffusion of information from inside an association to an exterior target or receiver information can be moved automatically or tangibly. Information leak risks typically happen through the web and email, although it can also happen through mobile information storage devices such as optical fibers, thumb drive, and PC. Information leak, also known as little and slow information stealing, is a vast problem for information safety and the harm caused to any association. Types of information leakage: -

Accidental breach: Unauthorized information leakage does not necessarily mean intended or malicious. An employee may unintentionally choose the wrong recipient when sending an email containing confidential information. Unfortunately, unintentional information leakage can still result in the same penalties and reputational damage as they do not mitigate legal responsibilities.

The disgruntled or ill-intentioned employee: Many information leakages occur through printers, cameras, photocopiers, removable USB drives, and even dumpster diving for discarded documents. While an employee may leak the information out of the building if they are disgruntled or promised a hefty payout by cybercriminals. This type of information leakage is often referred to as information exfiltration.

Electronic broadcastings with malicious intent: Association provides staff admission to the internet, email, and instant messaging as a portion of their part. The difficulty is that every mode is proficient in file transmission or retrieving exterior bases over the internet. Malware is regularly used to objective these modes and with a great accomplishment scale. Hackers could quite easily spoof a genuine business email account and request sensitive information to be sent to them. The user would unwittingly send the information, which could contain financial information or sensitive pricing information.

Insider risk: - It is a danger to an association that originates from persons inside the association like staffs, previous workers, freelancers or corporate connections who have confidential information about the association's safety exercises information and there are likely risks that the staff of the corporation may leakage the subtle information by error or meanly. The probable harm from leakage of credentials cannot be undervalued. The risk contains scam, the stealing of privacy or commercially valued information, the stealing of rational property, or the damage of system systems. It comes in three categories: -

Malicious insiders: The individuals who yield benefit of their access to inflict harm on an organization.

Neglectful insiders: The individuals who create mistakes and contempt guidelines, which place their association in jeopardy.

Infiltrators: External actors that obtain genuine access credentials without authorization.

Weak security passwords: - Employees use weak security passwords or easily predicted security passwords. This company uses cloud-based services that require different accounts. These services often can contain sensitive information and financial information. By means of easily predicted security passwords or the same security passwords for multiple accounts can cause the information to become compromised. For the ease of clients, occasionally functions do not impose password complication, and as an outcome of that, people use simple security passwords like admin, password123, 012345, name, own mobile number, etc. Weak security passwords do not always mean length and the characters used; it also means the predictability like Name !12345 looks quite a complex password but can be easily predicted. Creating a complex password won't serve the purpose if any employee writes it and sticks it on the desk.

Weaknesses in the existing system

The system within the company has an intrusion detection service that logs activity such as login attempts, web server and employee activities which is a small step towards security but this isn't enough as there's only one security engineer in the firm and it isn't possible for the engineer to keep track of all alerts and activities reported by the IDS and it is possible that the security engineer misses an activity or is late in responding or preventing an activity. The company could use an Intrusion Prevention System (IPS) that not only detects activity but actively tries to evade any malicious attempt made on the existing system. In an IDS, the system could log 1000s of activities in a day and the security engineer has no choice but to perform a daily or a periodical check on these activities by querying the data or looking at reports generated by the IDS (Eg: Splunk).

The workload on the security engineer is very high if we consider that they have to go through with keeping track of activities reported by the Intrusion Detection System, along with keeping a check on software updates on all desktops. The security engineer also has to periodically send out information security emails that other employees might not even read if it just involves information regarding safe security practices. This part could be improved if the periodic awareness emails are interactive and they involve questions that employees could answer but that doesn't reduce the workload on the security engineer. The workload would also mean that software updates and patches aren't implemented in a timely manner. The lack of security personnel is a major weakness in the existing system.

The company's premises have a few cameras installed in the office but that's about it. There are no cameras specifically placed in highly confidential areas like data centers or where physical assets of the company are housed, but they're randomly placed all over the premises. There is a security guard at the entrance to check IDs of employees and related people to get inside the premises but that alone isn't a great solution as people could use techniques like tailgating or bribing the guard to get in. They could even pay the security guard a few hundred dollars to go inside the premises in a particular room and steal a particular asset (a laptop or a hard drive) or even things like installing a rubber ducky. With only a handful employees in the firm, we can't expect the firm to have someone looking over the security footage and by the time such an activity is detected, it might be too late. It is important to have a biometric system on the entrance and everywhere possible or at least the entrances to offices, data centres and other confidential areas within the company’s premises and possibly personnel looking over the security feeds.

If we go back to the scenario, there was a security breach before which there were login attempts made on the admin’s account which resulted in a reset of credentials. This was possibly a brute force or a dictionary based attack that was successful in getting credentials of the admin and if the attacker did get access once, they would get access again unless there are substantial changes made to the password policy of the workplace. The attacker doesn’t have to get hold of the admin’s account but they can attack any particular system on the network and execute escalation privileges through various exploits and with that they can get access to the admin account or any account to support their malicious deeds. There is a need for a strict password policy that sets a minimum character length and asks for users to use uppercase and lowercase letters along with numbers and symbols.

Changes in the credentials would mean that the attacker cannot get access to the system through the credentials they used to get access, but that’s not necessarily the case. The attacker might have installed remote access trojans, spywares or keyloggers on the system on some other technique to maintain access to the system, a backdoor. There is a requirement of a thorough system check and the implementation of change/patch management, if applicable. The security engineer needs to pretty much dive into the system and look for any unwanted files as it could be hard to trace a backdoor.

The company doesn’t have a policy in place for employees that dictates how a personal device could be used, meaning employees could bring in their mobile phones and connect to the firm’s wifi and use it like they use their devices out of the company’s geographical perimeter. If an employee’s mobile phone is infected and then connected to the company’s network, it could spread to devices that are supposed to have important confidential files. They can access company information through their mobile phones which is unadvisable.

The company also doesn’t have policies in place that dictate their communication with other partnering companies or third parties they don’t know of. The partnering company could have severe security flaws that could be a problem for the firm in our scenario so it is important to communicate and know each and every detail about the other company that could come back to haunt the firm in scenario.

Employees are people and people can be a vulnerability. Every employee in a firm isn’t expected to be tech savvy and in our firm, there are employees that deal with governmental data that doesn’t have anything to do with technology or security. We cannot expect every employee to practice security measures if their job description doesn’t ask them to deal with technology anymore than logging data in spreadsheets on making reports on Word. An outside threat or an inside threat in the form of an employee can social engineer their way into getting passwords and possibly data that the firm cannot afford to make confidential. The target employee with less awareness and knowledge of cybercrime may end up giving that information to threat actors and unintentionally, put company’s credibility and resources at risk and these are the employees that threat actors generally exploit. Even the higher ups of the firm can be a vulnerability for threat actors to exploit. They can fall victim to various whaling and vishing calls.

Solution to Threats

It is necessary to be aware of new phishing scams by finding out about them as early as possible so that organization will be at a much lower risk of getting snared. Snapping on links that emerge in casual emails and direct mails isn't a clever attempt. A phishing mail might look like a genuine email and once a user clicks the link to the supposed website (cloned or another one altogether). The phishing email may ask an user to fill information, but the email may not contain your/organization's tag. Many phishing emails will twitch through "Dear customer,..." so employers should be aware when they come across these emails. Installing an anti-phishing toolbar runs a quick check on the sites that employers are staying and relates them to catalogues of well-known phishing websites. If an employer comes across a malicious site, the toolbar will alert them about it. Before submitting any form on a website, make sure the site's URL begins with "https" and there should be a closed look icon near the address bar and should check for site's security certificates as well. Not ever copy documents after doubtful emails or sites. Similar search engines may demonstrate evident links which might indicate to a phishing webpage that deals little price yields. If the person creates consumptions at such a website the card facts will be retrieved by criminals. High quality firewalls act as buffers between user and system and outside intruders. Users should use two different kinds of firewall: desktop and network. The primary is a software and following is hardware and once used collected they radically decrease the chances of hackers and manipulators penetrating systems and networks. Many popular browsers have a functionality that enables blocking pop-ups, if a user manages to slip through the cracks, don't click on the "cancel" button which may lead to phishing sites instead tick the "X" in the right-top corner of the window. Users should never share personal or financially sensitive information over the internet. Most of the phishing emails will direct to pages where entries for financial or personnel are mandatory. An internet operator must not ever create private admittances across the links offered in the mails and certainly not direct mail with perceptive information to anybody. By means of anti-virus software is always a good idea and always keeps the software up to date. Installing anti-malware is the best way to protect the system against malware attack. Anti-malware is planned to combat malware. It can similarly terminate malware before it influences the system. Anti-malware detects malware instantly by means of distinctive discovery gears and practices. It frequently examines the system to stop malware contamination. Anti-malware software protects the system against file-less malware. It moreover offers real-time defense in contradiction of malware, which means that it has the capability to inverse the loss the malware has completed to the system. There's a hazard in copying and mounting plagiarized software; they might comprise malware. A key system virus was coverage over an illegitimate replica of a software. Malware is frequently mounted over an infested copy. Many disregard scanning the URL or link, but this is unique of the finest customs to stop malware contamination. Malware is furthermore mounted over phishing links that produce bogus sites and webpages. Skimming the URL primary benefits confirm if the link is infested with malware or the system is safe. Developing a denial of the service response plan, systems specification. Progress a complete gradient of resources you must devise to guarantee innovative hazard documentation, valuation, and categorizing instruments, as well as security-enhanced hardware and software defense, is in house. Build certain your squad associates know precisely whom to reference in circumstance of the occurrence. Include the gradient of interior and exterior associates that must be learned about the occurrence. The company should also develop communication strategies with your customers, cloud service providers, and any security vendors. Secure Network Infrastructure can only be achieved with multi-level protection strategies in place. This includes advanced intrusion prevention and risk organization schemes, which chain firewalls, VPN, anti-spamming, filtering, harmonizing, and additional levels of DDoS protection methods. Composed, they allow continuous and steady network defense to avoid a DDoS outbreak from an occurrence. This comprises all from classifying imaginable traffic discrepancies with the uppermost horizontal of accuracy in obstructing the attack. Practice Basic Network Security Engaging in strong security practices can keep business networks from being compromised. Secure practices include complex security passwords that change on a regular basis, anti-phishing techniques, and firewalls that allow only restricted traffic to enter. These measures alone will not stop a DDoS attack, but they serve as a critical security foundation. Businesses should create redundant network resources; if one server is attacked, the others can handle the extra network traffic that would be directed to it in case of that attack. When possible, servers should be geographically spread. Spread-out resources are more problematic for hackers to target. Make use of the Cloud Outsourcing DDoS prevention to cloud-based service providers offering many advantages. One of the advantages is that the cloud has more bandwidth and resources than a private network likely does. This increases the magnitude of DDoS attacks, hence relying solely on on-premises hardware is likely to fail. Comprehend the cautioning ciphers roughly indications of a DDoS occurrence contain network strike, marked connectivity on a company intranet, or alternating website closures. Not all systems are faultless, but if an absence of routine appears to be lengthy or more austere than normal, the network probably is suffering a DDoS, and the enterprise should yield action. Considering DDoS-as-a-Service, it ensures that all the security infrastructure components meet the highest security standards and compliance requirements. To prevent brute force attacks, we need to keep these things in mind: password length, password complexity, limit login tries, modifying .htaccess file, by means of captcha two-factor authentication Cloudflare. Do not pay the ransom. Even if the ransom asked for is paid, there is no guarantee that files will be accessible or retrieved in the desired manner. If possible and secured, restore any impacted files from a known good backup. Restoration of files from a backup is the fastest way to regain access to information.

Do employ content scanning and filtering on mail servers. Inbound emails should be scanned for known threats and should block any attachment types that could pose a risk. One should make sure that all systems and software are updated at regular intervals with the most required patches. One of the most common methods used to spread malware is the exploited kits hosted on compromised websites. Regular patching of vulnerable software is a necessary step to help prevent the spread of this infection. If, by means of public wireless internet, make sure to use a trustworthy virtual private network when accessing the public Wi-Fi. The risk is real, and real risks need serious information leakage prevention. Information loss prevention is a strategy that ensures the end-users do not send any kind of confidential or sensitive information outside of the enterprise network. These strategies may involve a combination of user and security policies and security tools. DLP software solutions allow administrators to set business rules that classify confidential and sensitive information so that it cannot be disclosed maliciously or accidentally by unauthorized end users. Forcepoint DLP solution allows us to discover and control all sensitive information easily and identify your riskiest users within seconds. Never use a password related to name, place, or mobile number. Weak security passwords can be predictable, or the hacker can use brute force if a password is small in length, so one should try to use random strings with special characters. Though that can be hard to remember as a security point of view, it's quite secure. To restrict usage of sensitive data from employees, implementing COPE (companyowned personally enabled) policy is a good idea as it restricts employees from potentially harming the data intentionally or unintentionally in any way.

Cost and Budgeting

As mentioned in the scenario, the company's revenue is around $2 million dollars per annum and the CEO is willing to allocate around 9% of that to security which is around $180,000-$200,00 per annum. Since there is already a security engineer at the firm, we can deduct their salary of around $80k from the security budget that we have to work with. Let us look at the cost (per year) associated with existing security features and features that can be considered a part of the security infrastructure.

1. Intrusion Detection System - $8000
2. Biometric System (fingerprint)- $3000
3. Emsisoft anti-virus for 30 windows end-points - $600
4. Data Loss Prevention Endpoint for 30 end-points - $600
5. Carbonite cloud backup services for 50+ computers and 1 or more servers - $1000
6. 1 additional security engineer - $80,000
7. Mid range camera package installation including 8 cameras, 8 channel 1080P DVR plus labour and warranty costs for 2 years and two monitors to host live feeds - $2000
8. New phones and desktops (when required) - $5000
9. 3 year contract for firewalling (for a 25 employee business) considering there could be increase in number of employees in the future - $1500
10. Cable locks for hardware in the data center and offices - $800
11. Other costs - $10000

    The total implementation cost is **$112500** and when the income of the existing security engineer is added, the total cost comes to be **$192500** which falls under the allocated 8-10% bracket.

Summary

In this paper, we firstly identify the assets of the company in the scenario which included desktops, physical storage mediums and the company's premises. We also take a look at potential threats to the government contractor in the form of malwares and insider threats along with addressing gaps and weaknesses in the current security system including lack of personnel, poor password practices and lack of other resources like cameras and biometric systems. To counter these issues, we proposed solutions like enforcing a strict password policy, training employees, using Data Loss Prevention systems, Anti-viruses, Cloud backups, adding security personnel to the company and installing cameras and biometric systems to prevent unauthorized personnel from getting in the premises. We also have to keep in mind the cost constraints of a company as it's not realistic to implement every security practice possible if the company's budget doesn't allow us. We were given a budget of around $100-110k a year on security with an additional $80k on an additional security engineer and we were able to make significant changes to the current security architecture according to the budget allocated by the company's CEO.

Individual Contribution

Faraaz - Assets to be protected, currents weakness in the system and cost plan.

Aayushi - Threats to the company and solutions to those threats.

References

https://www.cybintsolutions.com/5-of-the-biggest-cyber-security-risks-for-businesses/

https://www.icaew.com/-/media/corporate/files/technical/business-and-financial-management/smes/bas-files/top-five-cyber-risks.ashx?la=en

https://bhconsulting.ie/computer-security-threats-solutions/

https://www.rutter-net.com/blog/5-ways-to-overcome-it-security-threats

https://www.computerworld.com/article/2582140/ids-products-and-prices.html

https://www.emsisoft.com/en/pricing/

https://tidbits.com/2018/02/07/carbonite-raises-online-backup-prices/

https://www.coxblue.com/8-cyber-security-best-practices-for-your-small-to-medium-size-business-smb/

https://www.costowl.com/b2b/time-attendance-biometric-cost.html

https://www.thumbtack.com/p/security-camera-installation-cost