**Question 1**. IT manager at XYZ Corporation

For this question it is assumed that XYZ Corporation is a firm that works in the medical industry that handles patient personal health information and insurance. Also, for the sake of illustrating the importance of the role of cybersecurity, it is assumed that the information involved more than 500 pieces of information leaked [1]. It is also assumed that the data lost is worse case scenario, unencrypted, and usable to the hacker.

While it has been harder and harder to attack a computer system in and of itself with advancements in technology, it is now more and more coming to light that a chain is only as strong as its weakest link. When it comes to computer security, it is proving to be the social engineering. A common way to use this attack on a company is called phishing. In fact, according to Stanford University’s paper, “The Psychology of Human Error Report” stated that “88% of all data breaches are a result of human error.” [2]. The World Economic Forum said that 95% of cybersecurity issues are from human related issues [2]. Phishing is defined by National Institute of Standards and Technology (NIST) as the use of convincing emails or other messages to trick a person into clicking on harmful links or downloading malicious software [3].

The impact at XYZ Corporation being medical is potentially quite significant due to the fact that we fall under Health Insurance Portability and Accountability Act (HIPAA), Centers for Medicare & Medicaid Services (CMS), and State guidelines. I mention these specifically because of the proverbial teeth behind each of these. For instance, HIPAA, each violation can cost upwards of $2,134,831 per violation [4]. This price does not include individual civil liability or other penalties. CMS can impose more and more restrictive and obtrusive inspections that can make day-to-day operations harder. Not to mention that CMS can modify, suspend or deny Medicare/Medicaid reimbursement along with imposing fines of their own [1]. As for the state, this can also have fines and risk of losing the ability to conduct business within the borders of the state.

**Risk Identification**:

According to Norton, there are basically 20 types of phishing attacks that XYZ Corporation needs to train every person in the company (lowest pay grade and volunteers all the way to the CEO) in. While knowing the names of each could be a fun way to gain recognition of some of them, which we will discuss more in the mitigation section of this assessment. It is more important to gain knowledge of the concept of what they are. Whether or not it is a generic phish addressed to whom it may concern to more of a spear phishing where the attacker has the name of the target, all the way to the attacker going after the CEO as in a Whaling attack. They basically involve an email or contact message of sort, trying to get the victim to accidentally click on a link or give sensitive information that the attacker can use. A good summary of the different types of phishing is presented in table 1. This information was gathered from Norton [5], along with the addition of one extra current threat since the publishing the use of QR codes [6].



Now that we have a brief understanding of what the attack on XYZ company was. Identification of what was considered sensitive in the data breach is of top concern. For HIPAA, this definition is any individually identifiable health information relating to an individual’s past, present, or future physical or mental condition, treatment for the condition or payment for the treatment [7]. Because of this, we must consult with our legal counsel to go through each piece of data to determine what would fall under HIPAA, as each individual infraction is considered its own violation. The risk associated with HIPAA to our company falls under four different tiers of classification: Unaware, Reasonable Cause, Willful Neglect with correction, Willful Neglect without Correction within 30 days [4]. Each classification has a different penalty range for our company. Compliance and transparency are very important for our company, which will also help to not only minimize the impact on our company’s brand, but also, HIPAA can impose not only civil monetary penalties but criminal and potential imprisonment as well. Minnesota State also has laws in place protecting its’ citizens when more than 500 people are involved in a breach, our company will have to coordinate with police to determine if we need to notify and coordinate with consumer reporting agencies within 48 hours. If they determine that the investigation needs more silence to catch the hackers, they can choose to extend this timeframe for us [8]. The next governing body that we need to notify is CMS. They will send a team to work with us to investigate what happened and how exactly the breach happened. Civil monetary penalties are potentially assessed by this body also. However, this body directly will impact our current and future Medicaid/Medicare reimbursement. Impacts of this magnitude without correction could be unrecoverable.

**Risk Assessment**:

To be thorough in our risk assessment, we will need to conduct a vulnerability assessment also. However, because we know this breach in specific was because of social engineering, it will be added for the sake of completeness and in good faith with working with the governing bodies that we are working to make sure that we are working hard to prevent future breaches.

As a healthcare company we will be dealing with a lot of data but here is a table of identified risks and their associated tolerance ranges to help in creating our risk profile for the assessment in table 2:



The likelihood of these risks being realized again is higher than normal due to the last successful phishing event. Now that the hackers have the name and e-mail addresses of one or more of our employees, it will be easier for them to conduct spear phishing instead of just generalized attacks. We can employ a couple countermeasures through our spam filtering software to attempt to lessen some of these attacks. But the human vulnerability will remain. Therefore, in the mitigation section, we will discuss ongoing steps to fix this.

**Risk Mitigation**:

Mitigating social engineering is a very challenging and changing goal post. I believe that XYZ company can be very successful though, by implementing a mandatory yearly awareness training campaign with on-going testing. We can get started immediately with training to become compliant with the requirements as soon as possible. We can outsource this training to a number of companies [9]: ESET cybersecurity awareness training, Hoxhunt, Phished, SafeTitan Security Awareness Training, Ironscales, Proffpoint security awareness training, Barracuda Phishline, Cofense PhishMe, Infosec IQ, KnowBe4. The benefit of utilizing one of these training sites is that they will have more convincing and evolving examples for the employees to look at increasing employee buying in. Croudstrike has made a mention that when employees look at a phishing incident as getting in trouble, they will increase the chances of the employee not wanting to report it, believing that they are risking getting into trouble. Instead of making this more into a potential point reward system, throughout the year, there will be random different fake phishing attempts sent to our employees. The employees are encouraged to look for these phishing attempts and report them to the IT department. When successful, they will collect points redeemable through the award system. The caveats for the training will be unsuccessful attempts. Too many of them will require more training with the potential to have to talk with the administration if the employee is completely uninvolved with the training. But having an extra bonus for finding a real phishing attempt.

**Risk Acceptance**:

When it comes to risk acceptance and patient medical information the sensitive information is too high to allow an acceptable risk amount for the digital data. The acceptable levels would have to be reserved for information that was not part of the core information that could be linked to what would be covered in HIPAA, CMS, and State statute. For instance, insider threat. With proper vetting and company policies for HR review I believe that the risk can be kept to a acceptable level

**Risk Transfer**:

Since we have established a mitigation plan to prevent future breaches from phishing attacks, I believe that another attack is still possible, due to the nature of the sophistication of phishing due to the use of AI. I believe that we should investigate getting insurance for residual risks for any unforeseen risks that evolve in the future.

**Question 2** CISO at SafeBank Corp

Thank you, board of directors, for your time today. There has been an increase in threat levels emerging, so much that has reached the level that will require investing in upgrading of the network. Combating the surge in cyber threats of ransomware attacks at SafeBank Corp is of the utmost priority for stakeholders to ensure that we don’t risk the reputational damage and loss of confidence of our customers due to a ransomware lockdown. A 2024 report from Rapid7 said that ransomware payments have topped $1 billion [10]! The initial concerns brought to my attention from the board were also confirmed by the Microsoft Digital Defense Report 2024. In that report, Microsoft has observed that there is indeed a 2.75x increase in ransomware encounters [11]. Also, in the report went further in saying that “more than 90% of cases where attacks progressed to ransom stage, the attacker had leveraged unmanaged devices in the network” [11]. Because SafeBank Corp has been utilizing some legacy devices for the network, this will require a secondary report that will be at a follow-up meeting, once a full analysis of our network structure can be completed and a list of devices that need to be upgraded, along with the final costs involved. The rest of this report will address what we are facing threat wise, along with a detailed overview of how SafeBank Corp can be a leader in the industry and protect our valuable and well-deserved reputation through the years.

**Risk Identification**:

Ransomware is easily introduced to the network through multiple channels. Table 3 summarizes the main ways in which SafeBank Corp needs to prepare to protect against.

|  |  |  |
| --- | --- | --- |
|  |  | Table 3 |
| Phishing Emails | Attackers send e-mails with malicious attachments or links to ransomware [12] | |
| Remote Desktop Protocol (RDP) Exploits | Exploits using weak or misconfigured RDP settings, gain access to systems and deploy the ransomware [12] | |
| Software Vulnerabilities | Unpatched software, outdated, or unsupported systems provide entry points for ransomware [12] | |
| Dive-by Downloads | Visiting a compromised or malicious website can trigger a ransomware download | |
| Malicious Advertisements (Malvertising) | Ad networks on legitimate websites serving infected ads [12] | |
| Compromised Credentials | Weak or stolen credentials [12] | |
| Malicious Third-party Applications | Pirated software containing malicious code [12] | |
| Fileless Attacks, Zero-footprint Attacks | Fileless malware uses a computer system’s built-in tools to execute a cyberattack [13] | |
| Malware Obfuscation | Transforming malicious code into a different format to hide from security tools [12] | |
| USB drives | Unknown, found, USB drives plugged into networked devices containing malicious code [14] | |
| Ransomware-as-a-Service (RaaS) | A cybercrime business model where ransomware operators write software, and affiliates pay to launch attacks using said software [12] | |

These entry points are vulnerabilities that the next Table 4, will classify as priority and who can affect them the most (own them).



**Risk Mitigation**:

The best part of Table 4 is when it comes to the end user employee responsibility. This will come down to an education campaign that can prevent the majority of SafeBank Corps’ risk of exposure to ransomware. The initial education campaign will need to be companywide learning about phishing. As creating educational material including interactive video content, example e-mails, and testing would take a lot of time and resources. I believe it is more cost effective for SafeBank Corp to outsource this to a third party. With the board’s permission I would like to begin contacting multiple existing companies to obtain quotes for this service. What will be needed is annual training about phishing. Then, ongoing diligence of the employees by having random test phishing e-mails that they can report to the IT department through our existing outlook reporting system. Through the IT department, we can also assist with limiting true phishing emails that get through to the employees through using good security practices and policies built into MS outlook filtering systems and filter as many as possible at the gateway. Another annual training will need to address general safe internet safety. Looking at some of the phishing educational sites, many offer training of this included. What we can do in the IT department to help, especially since October is Cyber Awareness Month. Is help increase awareness in common penetration techniques. One red team technique is to put random USB drives around where employees can find them. These USB drives have code on them to allow the pen tester to get into the target network. I know, reading this, no one would believe that something like this could be so simple, or effective in breaking into a network. But we can ask Iran how effective it is. Without having to go too far into details and bore the board. Basically they had a really secure system that wasn’t even attached to network (air gapped) and yet the Stuxnet worm was able to get into their system and destroy their centrifuges. This was accomplished using a USB device! If anyone on the board would like I can provide the individual with links if they would like to read more into this. It was huge news, people denied who was responsible, big controversies and such. But, unfortunately, the reason why I am talking about this to the board is because. If a big governmental, super secure, area can be penetrated by a simple USB. I believe, we could be at risk without simple training. Another potential step SafeBank can take is to have IT disable any unused USB port on our desktops.

The Software Vulnerabilities are a high priority. What also makes it harder for SoftBank is because there are also some firmware problems for our company. SafeBank has some older software and devices that are no longer supported by the manufacturer. Upgrading the software and networking devices will be a capital investment, but a critical one.

As for the threats marked for IT. We are working on implementing an automated system to make sure that patches are pushed through to the systems as soon as they become available to our supported systems. Once we have upgraded the systems needed, SafeBank Corp will have 100% compliance with this goal. IT has been tasked with updating access control and designing a network segmentation structure. This report will be completed and presented to the board by the head IT manager at the next board meeting. As I am new to the company, I have recently been made aware that we did not have a disaster recovery plan. I was told that because we use the cloud for our backup that it was believe that it was “taken care of”. By the next board meeting, I will have a plan drafted and ready for approval by the board. I also believe that we need to add an offline backup to our system. This is recommended by Cybersecurity and Infrastructure Security Agency (CISA). CISA has made a stop ransomware guide that I have made into a checklist that I will share with the board but have also made into a separate checklist that I sent to the head of the IT department to assure that we are compliant with these best practices [15].

* Do not expose services, such as remote desktop protocol, on the web.
* Conduct regular vulnerability scanning to identify and address vulnerabilities.
* Regularly patch and update software
* Ensure all devices are properly configured and security features are enabled
* Limit the use of remote desktop services
* Implement MFA on all VPN
* Require passwords of more than 15 characters
* Consider subscribing to credential monitoring services
* Implement identity and access management systems
* Implement zero trust access control
* Change default admin usernames and passwords
* Do not use root access accounts for day-to-day operations
* Enforce account lockout policies after a certain number of failed login attempts
* Store passwords in a secure database and use strong hashing algorithms
* Disable saving passwords to the browser in the group policy management console
* Implement local administrator password solution
* Don’t allow reusing passwords
* Use windows PowerShell remoting, remote credential guard, or RDP with restricted admin mode as feasible
* Separate administrator accounts from user accounts
* Enable common attachment filters to restrict file types that commonly contain malware
* Implement domain-based message authentication, reporting and conformance policy and verification
* Ensure macro scripts are disabled for MS office files transmitted via email
* Disable windows script host
* Use automatic updates for antivirus and anti-malware software and signatures
* Use application allowlisting and/or endpoint detection and response solutions
* Implementing and intrusion detection system
* Monitor indicators of activity and block malware file creation with windows Sysmon utility
* Implement protective domain name system
* Apply the principle of least privilege to all systems and services
* Employ logical or physical means of network segmentation
* Restrict usage of PowerShell to specific users on a case-by-case basis
* Secure domain controllers
* Retain and adequately secure logs from network devise, local hosts, and cloud services
* Establish a security baseline of normal network traffic and tune network appliances to detect anomalous behavior
* Conduct regular assessments
* Enable tracking prevention
* Enable website typo protection
* Enable browser-based AV
* Block website notifications by default

I have requested the head of the IT department to go through this list made available for us and check off what we have. What can be done with existing equipment. What is not feasible without more equipment, with of course a written proposal for the board for said equipment. A strong point to end with for our company is that we don’t have a network that is only one operating system that would allow for easier propagation of viruses and hackers. Our network is a combination of Microsoft and Linux servers.

**Risk Response**:

Risk response for a successful ransomware attack is best outlined by CISA in the StopRansomware Guide [15]. There is an actual checklist that has been created that just needs approval by the board. I made a copy of this checklist [15] here for completeness of this report. But I have also made a separate file with complete details for further review by the board for approval.

1. Determine which systems were impacted, and immediately isolate them.
2. Power down devices if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.
3. Triage impacted systems for restoration and recovery
4. Examine existing organizational detection or prevention systems and logs.
5. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.
6. Initiate threat hunting activities.
7. Follow notification requirements as outlined in your cyber incident response and communication plan to engage internal and external teams and stakeholders
8. If the incident resulted in a data breach, follow notification requirements as outlined in your cyber incident response and communication plans
9. Take system image and memory capture of a sample of affected devices
10. Consult federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available
11. Research trusted guidance
12. Identify the systems and accounts involved in the initial breach
13. Based on the breach or compromise details determined above contain associated systems that may be used for further or continued unauthorized access
14. If server-side data is being encrypted by an infected workstation, follow server-side data encryption quick identification steps
15. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms
16. Rebuild systems based on prioritization of critical services
17. Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility
18. The designated IT or IT security authority the ransomware incident over

**Risk Monitoring and Review**:

Now that we have gone through a large list of additions, modifications, policy changes, and strategies. I believe that we will be set to combat this emerging threat to our company. Due diligence will make it necessary for everyone to buy into the annual training and watching for the latest social engineering schemes that will be presented to everyone. As for the IT department. I believe that the new system with intrusion detection software, combined with the established security baseline of normal network traffic and network appliance notification of anomalies, will go far in assisting with monitoring not only this threat but many unforeseen threats that will develop the future.

**Question 3** Security Architect for TechSecure Inc

TechSecure Inc has taken on a very challenging task of securing our smart home product. With the growing threat posed by a juicier and juicer target. Statista has predicted that three will be 39.6 billion IoT connections worldwide by 2033 [16]. As any company wants to thrive in the market. TechSecure needs to learn from the mistakes of other large companies. Take Ring Home Security for example. Their data breech led to dozens of lawsuits due to hackers getting into 15 family’s devices and harassed the family members [17] [18]. Another one that TechSecure needs to really look at is the Nortek Security and Control access control system Breach. May 2019 Applied Risk identified 10 high risk vulnerabilities [18]. This initial report I found was completed in 2021 noting the data breach caused by the vulnerabilities [18]. A second report that was discovered was much more concerning this breach. Securityweek released an article March 2024 stating that the “vulnerability was patched 5 years after disclosure” [19]. Publicity of that nature is something that TechSecure Inc needs to stay far away from for certain. Other scary things that TechSecure can potentially market against would be keeping our customers off the “Raptor Train”, a botnet that was discovered using more than 200,000 IoT devices worldwide [20]. With that being said, the threat model will be broken down into the following components Asset Identification, Attack Vectors, Risk Assessment, Mitigation Strategies, and Continuous Monitoring.

**Asset Identification**:

Bitdefender released a 2023 report gave a listing of approximate percentage of what is found in the smart home ecosystem, the numbers follow [21].

* Smartphones 40.9%
* Computers 16.2%
* Streaming Devices 14.6%
* Tablets 8.8%
* Smart TV 5.4%
* Console 4.2%
* Other 9.9%

The assets that we need to defend that are considered the most vulnerable per this report [21].

* TV 52%
* Smart Plug 13%
* Router 9%
* DVR 8%
* Extender 3%
* IP Camera 3%
* Set-Top Box 3%
* Media Player 3%
* NAS 3%
* Home Automation 3%

The percentages listed are of the identified vulnerabilities by Bitdefender [21]. That is what effected each of those systems.

**Threat Identification:**

The challenge here for the threats is that the threat actors have deep pockets. Some of these are government sponsored threat actors. For example, the Raptor Train mentioned in the introduction is believed to have originated in China [20]. The majority of products for homes will be on a flat, unsegmented network, based on what NIST has said about the underutilization of network segmentation practices. Getting survey information about precise numbers is hard. What I have found is a 2019 study by consumer reports of 1006 American adults resulted that only 38% of someone saying that someone had changed the default password for them [22]. This being said, there is a high likelihood that the only thing protecting TechSecure Inc’s products is a router with potentially a default admin password active. Here is a listing of some potential IoT security threats of note:

* Use of Default Passwords [23].
* Unsafe communication, unencrypted [23]
* Automation and AI, with no checks [23]
* DDos attacks [24]
* Botnets [24]
* Zero-day IoT vulnerabilities [24]
* Ransomware [24]
* Miners [24]
* DNS Changer [24]
* Proxy Bots [24]
* Spying on owners via webcams, Privacy Concerns [24]
* Physical safety risks, ex door locks [24]

**Attack Vectors**:

There are two main attack vectors that are noted that we need to defend against per Kaspersky. The two routes are Brute-forcing weak passwords and exploiting vulnerabilities [23].

**Risk Assessment:**

According to Bitdefender Denial of Service is 84% of all the recorded incidents that was recorded in 2022 [21]. Table 5 shows the list of threats with the risk level and the potential of exploitation rated using the 2023 Bitdefender security landscape report [24].



**Risk Mitigation:**

In researching the problems associated with the IoT security. NIST and many other sites have mentioned that many devices are not securely configured by default from the manufacturer. I believe that this would be a great starting point for TechSecure to begin. Much like companies needing to invest in combating social engineering by teaching their employees how to recognize it and how to stop it. I believe in becoming a leader in teaching our customers how to secure their home through simple videos, for example. Easily sharable, but also able to spread the brand name out at the same time, free marketing.

All TechSecure products need to have modifiable administrator usernames and passwords. Having the customer be required to change the default password after the initial startup would be another way to prevent brute force attacks to be easily successful. This will be a great way to address the risk of using and keeping the default passwords.

To avoid the unsafe practice of unencrypted communication. TechSecure could make secured communication the default setting.

Automation of setups or setup with AI assistance can be a double-edged sword. At TechSecure, using a double check process before releasing new updates to the wild may be a way to prevent this from happening to our products.

The next nine risks can be addressed at the same time. As securing against one will help to secure against many of the others. The home network needs to be updated from flat networks. Having a segmented network will not only make it more secure for the customer. I believe that they will also enjoy the potential speed increase due to not having a much network traffic from say the refrigerator. This, of course, puts more work on a router which will need to have updates completed automatically by default. TechSecure also needs to have their routers have firewall setups as a default. All products need to secure boot.

**Continuous Monitoring:**

Continuous Monitoring in a customer’s home through an annual subscription service would be a way for TechSecure Inc to be able to accomplish this task. Part of the software suite would need to have an intrusion detection software installed. To keep up to date with all the patches that will come up throughout the life of the products. The customer will need to agree to keep the auto update enabled. For every new product that the customer purchases and adds to the subscription service a vulnerability scan should be conducted, along with a yearly scan on the anniversary of the customer’s start date. For additional security, the customer could purchase different levels of a penetration test through a contracted company. With this subscription service in place, it would enable TechSecure to respond to a potential real-time threat when the intrusion detection system sets off an alarm.

**Risk Acceptance and Transfer:**

Because of the nature of working with customers and an ever-evolving state sponsored threat. It is impossible to prevent all breaches. Because of this, with taking all precautions that can be foreseen. Looking into cyber insurance for the remaining risk is at an exceptable level.

**Question 4** Global Electronics Inc

Given the current geopolitical climate in the USA, this question has become a very tough question to mitigate. As an electronic component supplier it is probably not possible to get all components from at least two different suppliers. So, implementing a double redundant system is probably not possible or financially feasible. That being said, applying the methodologies learned in class can still be used to attempt to minimize the effects of the threat showing that risk management training techniques in the computer world can be actually multi-disciplinary and used in all businesses.

**Risk Identification:**

A list of the potential threats to the supply chain was provided in a report from Moody’s [25] and is listed here:

* Poor supplier performance
* Demand planning complexity
* Global labor shortage
* Rising inflation
* Volatile global economy
* Complex regulatory environments
* Geopolitical risk
* Reputational risk
* Natural disasters and climate risk
* Cyber risk

**Risk Assessment:**

Table 6 illustrates the current perceived risks that Moody’s identified.



In the recent past CNN news reported that there was a supplier issue with components to make electronic components [26], this is why it was rated medium. I am not aware of any imminent pandemic lockdowns to cause the demand planning complexity, so it is low currently. The same with global labor shortage. Rising inflation is at high risk currently and is all over the news. Along with a volatile global economy, complex regulatory environments, and geopolitical risk. Multiple mainstream media posts have made mention of this. Unfortunately, it is similar to reputational risk even if some of the later risks were not at high risk, because of the effects of media, I believe it would still need to be taken into account. However, for actual reputational risk. In good faith the company brand remains untarnished and away from things like what happened with Bud light. I believe the reputational risk is, actually, low. National disasters and climate risks are medium this time of year due to hurricane season and need re-evaluation throughout the year. Cyber risk is a persistent threat that will always be there and I don’t believe can be lowered below a medium risk even with the best care due to zero-days and being a large company meaning large target.

**Risk Mitigation**:

Poor Supplier Performance: The best way would be to use the age old saying don’t put all your eggs in one basket. Attempt to have multiple sources of each of the components needed to produce our products. Moody’s recommends watching the supplier’s financial health as a predictor also [25].

Demand Planning Complexity: This was emphasized during the covid pandemic when how much of each item needed was harder to predict. Because it is marked low at this time, staying with the historical increase prediction models should be alright. If at any point in time that this would need to be marked high risk again. Then Moody’s recommends a more sophisticated algorithm [25].

Global Labor Shortage: Components needed to make the electronics is marked low at this time. Having multiple suppliers could help mitigate this risk if it becomes a higher potential.

Rising Inflation: This one would need expert consultation at it’s easiest. Weathering the storm through the next upcoming months should help as this one has been tied to the geopolitical risk and political uncertainty that is currently going on in the country. Mitigating this will potentially have made longer-term contracts helpful in this situation.

Volatile Global Economy, Complex Regulatory Environments, and Geopolitical Risk: Mitigation of these is all tied at the current time due to the political climate. Needing to wait on if tariffs are going to be imposed at extreme levels or not. In general, having an expert group of financial analyzers and diversifying both onshore and offshore suppliers is a way to help navigate this current situation according to Moody’s [25].

Reputational Risk: Avoiding taking sides in hot button topics in current media climates. Utilizing advisors to watch for neutrality should help. A list was created by a company called Reputation911 to assist with this area [27]:

* Develop a crisis management plan
* Monitor your online presence
* Encourage transparency
* Prioritize ethics and compliance
* Train employees on reputational risk management
* Foster strong relationships with stakeholders

National disasters and Climate Risk: Strategic placement of where Global Electronics Inc. facilities are located with disaster planning for alternate routes for supplies to be delivered will go far in mitigating this threat.

Cyber Risk: Investing in having strong CISO and following NIST guidelines will help mitigate this threat.

**Risk Monitoring and Review:**

Continuous monitoring can be accomplished through using an asset tracking program. Instead of using an information system, ITAM, obtaining a specialized one for logistics would be the best option. Forbs.com provided a list of ten software suppliers for Global Electronics Inc to research and obtain pricing bids for. The 10 are listed as follows: Shippabo, Magaya Supply Chain, FreightPOP Transportation Management System, Precoro, Spplier Chain Management Software by Intelex, Logiwa WMS, NetSuite, Epicor Kinetic, Anvyl, Tada [28].

**Contingency Planning:**

Contingency Planning for the my top three ended up needing to be my top four. Rising inflation, Volatile global economy, Complex regulatory environment, and geopolitical risk. With the current political environment there would be very real chance of these four risks coming to fruition and needing to be delt with.

Being proactive on these could help Global Electronics Inc to weather the storm instead of actually waiting for the potential of the risk being realized.

Volatile Global Economy: Moody’s recommends managing any financial risks that Global Electronics Inc directly controls [25]. Consulting with economists and the board of directors to determine where they are willing to take the risks will aid in this area. Potentially investing in an electronics recycling facility to recover the materials used for the unsold products on our wholesale side. On the suppler side. Having multiple different suppliers to be able to negotiate and re-negotiate materials would be helpful.

Complex Regulatory Environments: the risk of tariffs has been stated in the news. If this is realized moving the facilities back to the states would be the simple solution. That being said, many products require components that need to be imported. If that is the case, then potentially talking with the current administration at the time to see about getting a special exception to the new tariffs would be feasible.

Geopolitical Risk: With the real chance of areas that supply routes will go by a war area. A meshed network for routes would be ideal if possible. Here again having more than one supplier would be ideal.

Rising Inflation: Moody’s recommends diversifying supplier relationships to help distribute rising costs [25]. Forbes recommends leveraging technology to cut costs [29]. Foley recommends revisiting and use provisions in existing agreements to work through the rising costs [30].

The final plan that Global Electronics Inc needs to establish an insurance plan to cover the remaining risk. Having a comprehensive risk management plan should go a long way in negotiating a better insurance premium.

**Question 5** TechSavvy Solutions

The development of an effective ITAM solution is essential for large businesses to survive. In class it was illustrated how it can optimize not only cost and budgeting. But it can help with risk reduction, optimization, future planning, and overall lifecycle management of equipment. With a project of this scope. Proper Planning before implementation is key. With a large company seeking an expert advisor would be beneficial. For a small company that is not able to afford something like this, taking a through approach for the asset manager to not only can justify maintaining the current position but also can establish the importance of the position of asset manager with being able to show quantifiable money savings and potential legal protection.

Mara Zeldin from Alsbridge created a “roadmap” for the steps in creating an effective ITAM. The roadmap breaks the process into three blocks [31]. Inventory, Contracts and Finance, and Software compliance [31]. As with any project, upper management and boards like to have timelines. In this article it recommends three to six months for the initial activities which include [31]:

* Identify inventory tools, database ad auto-discovery tools [31]
* Basic setup of ITAM policies and processes [31]
* Establish ITAM operating model [31]
* Initial asset inventory baseline [31]

After this phase in the implementation of the ITAM longer range goals can be planned. These goals according to Mara are hardware contract data integration, finance data integration, and software compliance [31]. While in business it can be risky to put timelines on a project. Careful consideration of the business environment at TechSavvy Solutions would need to be added into the equation for a more accurate estimation.

**Asset Identification**:

Being TechSavvy Solutions relies so much on the technology for daily operations. This report will need to include not only standard office equipment technology like desktops, laptops, and BYOD’s, but also lean heavily on the network infrastructure side.

**Asset Inventory**:

Assets to be considered in scope of inventory for this ITAM will need to include any hardware that the company uses that connects the network in a business manor. This would also include technology that doesn’t directly connect but instead relies on interactions via human input. Because of the need to track this will also need to include a temporary asset of the BYOD that the employees bring.

All software/firmware needs to be included in the scope of the ITAM to protect the company against risks to be discussed later under risk management.

A complete list will be created and maintained of all the firewalls, routers, switches, hubs, network appliances, and servers. This list should also include the testing equipment that the company owns to maintain such equipment. It is easy to forget about the Fluke tester can run into the thousands of dollars.

I would propose creating or purchasing of a database that had the capability not only dynamically keeping track of the inventory, but also one that reports could be run to give the company updates as to when products are expected to be end of life, or licenses need to be renewed. While there are a lot of companies that offer a product that will do this and provide capabilities for future growth. Sometimes it is not in the budget to purchase one of these databases in the initial stages until justified and approved further into the development of the ITAM. Something as simple as utilizing Access in the Microsoft Office suits that many companies already have. A quick internet search for a sample inventory database could be beneficial in gathering information while keeping it relevant during the initial phase. Along with providing a way for the information, it will be able to be ported into the more robust system that will be put in place after implementation of the ITAM.

**Lifecycle Managemen**t:

Procurement phase

Initial procurement of essential networking needs to go through extensive planning in the conceptual phase involving the IT department and the upper management to better match the overall mission of TechSavvy. The following areas need to be taken into consideration when going through this phase is identifying the reason to get the asset. Whether it is to replace an existing asset or to expand [32]. Once decided on the equipment needed the procurement phase can progress to working with different venders to get the best price/service mix determined in the previous phase that will overall benefit TechSavvy long term. Building a list of suppliers can sometimes help in the negotiation process.

Maintenance/utilization Phase

Ideally, this phase is the longest phase. For this to occur routine maintenance of the assets needs to be scheduled and accounted for. According to Emaint, “the focus should be on extending the asset’s useful life and maximizing productivity, while keeping costs low” [33]. This can also maximize uptime by scheduling preventative maintenance and predictive maintenance [33].

Disposal

At the end of asset life, sometimes the company can recuperate some of the costs of owning the asset. One way is potential resale to another company that could use the item. Different types of recycling programs will pay for items if sales is not an option for the asset. This of course is after all security measures have been followed, assuring that there is no risk of a data breach or other forms of corporate espionage.

Following the best practices of the asset lifecycle management will lead to more optimal use by keeping the product uptime as high as possible. Along with going towards aiding in cost-efficiency by reducing unplanned down times [33].

With this being said. This is why lifecycle management is diagramed as a circle. Proper planning a head of asset failure/obsolescence will keep TechSavvy Solutions up and running.

Replacement planning phase to circle back into the procurement phase above.

**Risk Management**:

Once TechSavvy Solutions has a working ITAM application of the Stride Model, it will assist in helping with the security issues that they have been having. Having a dynamic database of assets available it will be easier for intrusion detection systems to monitor for new devices and spoofing. When it comes to the BYOD using keys and MFA can assist watching for deviations from patterns of employee device utilization. This being said, it wouldn’t be unreasonable to have in policy of notification when the employee changed phones or carriers for example. This also will allow for watching for shadow IT systems in the process. BYOD has multiple other potential risks that also need to be addressed separately from just spoofing. At the end of the standard Stride Model an additional list of potential risks with BYOD is listed followed by what ITAM potential can assist with along with what will need to be addressed with policy and IT assistance.

Tampering can be controlled by records of access to all data that belongs to TechSavvy Solutions. This blends right into Repudiation. Digital signatures, access records and devices used will go a long way in keeping everyone honest knowing that everything done on the network has a record taken of that action.

Information disclosure will be greatly assisted with an ITAM. Routine reports can be generated of devices that have not been auto updated with the latest security patches for follow up with IT.

Denial of Service will be also fought against with ITAM. Patched, properly configured networks will aid in lowering the chance of a successful DDoS attack. This is along with annual trainings for all employees against social engineering attacks.

Elevation of Privilege can also be grouped in with DDoS attacks. ITAM can assist in the same way by keeping records of all users. Including how often administrative users are being used and what is being carried out under the Sudo or Root user.

BYOD security risks. Posing a unique new and emerging risk to companies that have many potential benefits when handled correctly and addressed with proper security and policies. Teramind addressed this by giving a blog post about eleven potential security risks [34]:

* Data leaks through convenience mistakes
* Malicious insider threats, due to devices not connected to a central monitoring network
* Compliance enforcement
* Stolen/Lost Devices
* Malware
* Mobile device management gets hard with non-company owned equipment
* Email Exposure, sending wrong e-mails through wrong accounts
* Insecure data transfer with USB devices
* Lack of employee training in best practices when using BYOD for company business
* Insufficient BYOD policies
* Mixing personal and Business use on the same device can lead to complacency with items like credit card numbers from personal use vs company use

ITAM can assist with the BYOD security risks that TechSavvy can and will experience. But it will require a combination of good IT security policies and company user policies that will be needed in tandem with ITAM for mitigation of this list. ITAM can help with repudiation with all the outcomes of these mistakes. With dynamic asset accounting, ITAM can assist with guarding against spoofing and tampering. Information disclosure, the user training and policies will be key. Potentially limiting what types of BYOD that the company allows will mitigate the threat of a dangerous USB being plugged into the network. Policies with frequent training to guard against complacency can assist with the mistakes caused by mixing business and personal lives on one device.

**Monitoring and Reporting**:

This area is where ITAM truly shines. Monitoring for unusual deviations from normal network traffic will be much easier to detect with a good ITAM. As discussed in the risk management section ITAM can monitor a great number of threats that TechSavvy will face. Reports will be key to helping TechSavvy watch its internal money utilization and data loss prevention. Not only do ITAM companies always bring up useful reports that can be run for the board for annual expenditures and uses for predictions and such. But ITAM can also generate reports for regulatory bodies when requested for audits and post event investigations [35].

**Policy Development**:

Policy will be needed to have a process for adding, maintaining, and removing old assets. Yearly training updated to include more training identified as potential weak areas where the human component could introduce a risk of social engineering. Policies for what types of bring your own devices need to be developed with expert consultation from IT and legal, along with what the consensus of the board is. Contracts and legal paperwork need to be developed for acceptable use policies for BYOD. Policy for how to register with IT when a employee is going to use their personal phone for example with mechanisms in place for if the device is lost stolen or damaged beyond use. Policy needs to be considered if IT is going to service BYODs also.

**Question 6** HealthTech Solutions

HealthTech Solutions is venturing into an area of the market where the rules and regulations get very muddied and each hospital employees a legal team to provide their best interpretation as to what they believe will keep them safe in court as not all areas covered in HIPAA, for example have been challenged in court. This has led to inconsistencies in between hospitals and inefficiencies in processes because of this alone from personnel. Experience. From personal experience as a paramedic, I would bring a patient to an ER in the city I live in. Registration would of course meet me at the door to get the patient admitted into the system and get the chief complaint so EPIC had a starting point for the patient encounter. After I finished my report to the doctor or nurse, I would have to go back to the same registration person and get the “face sheet” this sheet contained billing information needed to complete my run report and to be able to tie it into the patient’s permanent record. And the inefficiency that was at that time was that the registration person would print the sheet for me, but before handing it to me, needed to take a black marker and cross out the patient chief complaint for that visit. The chief complaint was of course what I just informed them of and was my field diagnosis. This of course took extra time for the registration person, especially during busy times where they were trying to manage multiple other things at the same time. When it was very busy or if I had other calls pending, I would have to have them fax it to dispatch for me to collect at a later time so I continue to the next patient in need. This led to the next inconsistency, and also what was determined after review, risk. When they faxed it to dispatch they didn’t need to redact the chief complaint information. Even though it was being sent to an area where it was secured, but readily readable by the random people in dispatch. The same document with the hospital across the city did not require redating when given to the paramedic that was directly involved with the patient, but redacted the information when sending it to dispatch. I took time to mention this as an example of how muddied the waters are with HIPAA and how hospitals choose to handle the data.

Data Creation

Data creation is the best time to start the process of securing the data and assuring the CIAA triad. Each choice of data types should have format enforcement for quality control. Metadata management should also be strictly enforced. Because we are dealing with a complex, however a database at its core. We need to insure that identification key fields are complete to ensure that each record is placed correctly.

Data Storage

Data storage for a database of this size will require large investments. HealthTech Solutions board will have to decide if they want to store the primary data onsite or in the cloud [36]. This will need to use the most current encryption options available and updated when it is found that a new version is proven better. As for the new threat of encryption breaking by quantum computing, this will need to be addressed at a later date when a solution is publicly available. As with basic IT training, mission critical data needs to be stored in at least two different locations. Daily backups need to be completed to what would be preferred to an immutable [36] form of storage to greater assist in the integrity portion of the CIAA triad. This can be of different types of SSD or tape [36].

Data storage will vary as to how long the data will need to be stored based on multiple factors. As the company grows this will also need to be readdressed. For instance, HIPAA leaves the majority of patient information storage to individual state statue. For the small accounting part that is mentioned it is 6 years from creation or when the information was last in effect [37]. From experience, the companies that I work with that work across state lines default to the state with the strictest rules. As HealthTech Solutions is rapidly growing it might be of benefit to look at all 50 states including territories and the District of Columbia to find the longest times of all of them and compile a length of time for records from that list.

Data storage with confidential health information needs to be secured in locked rooms with recorded access control.

Data Maintenance

Regular monitoring and maintenance needs to be completed to ensure integrity of the data. Having the data it two different areas allows for cross comparison for damage and alterations.

Data Usage

Data that is not available for access when needed is not of use. Accessibility in the CIAA triad can be accomplished by using VPN access to cloud storage after multifactor authentication.

Data Sharing

Protocols for sharing will need to be discussed with each and individual client as to what they want shared for what level and what forms are needed to be signed along with how long they are in effect for. For instance, Care everywhere can be accessed through EPIC. When we fill out the initial form. Many of the other hospitals choose not to disclose the patient's mental health with the initial form. A separate form needs to be submitted and signed to obtain that information. This will leave a large area for HealthTech Solutions to provide audit trails for all of the non-digital paperwork that is added to the mix of the digital medical record.

Data Archival

Highly sensitive data can require multiple types of back up. Continuous back up would be one to start with but, in the cases of things like ransomware they can easily be destroyed also. So using continuous as a first backup is a start. But then implementing either a daily back up or a back up triggered when a certain amount of data is added would be a second, followed by a rotating weekly backup stored off site. All forms would need to remain encrypted [36].

Data Disposal

After the lifecycle of the storage asset has been reached. Following NIST SP 800-88 for proper disposal of the devices is critical to security. Ultimately, depending on the type of media. Contracts for the pulverization or degaussing will need to be obtained. To complete the lifecycle NIST recommends adding documentation record of the process including these items [38]:

* Manufacturer
* Model
* Serial Number
* Organizationaly assigned media or property number
* Media type
* Media source
* Pre-sanitization confidentiality categorization
* Sanitization Description (clear, purge, destroy)
* Method Used
* Tool used (including version)
* Verification Method
* Post-sanitization destination
* For both sanitization and verification
  + Name of person
  + Position/title of person
  + Date
  + Location
  + Sign

Monitoring and Review

Monitoring and review will be conducted using the in place ITAM. Review of these policies should be completed with every new client added. With a full review for updates and best practices at least yearly.