

The two biggest security recommendations that I would make for Company X for students to securely access applications, files, classes, along with reducing the success of phishing attacks, and protecting college networks would be:

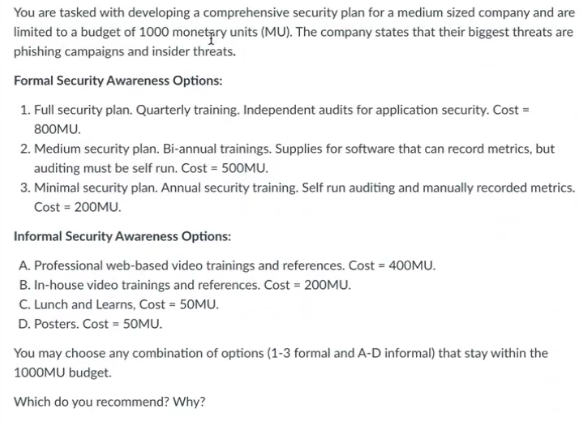
* Multifactor Authentication + Virtual Private Networks
* Email Protection: Link Scanning, Attachment Scanning, and External Domain Headers

Regarding students securely accessing applications, files, and classes, I would have Company X implement Multifactor Authentication, along with Virtual Private Networks. Multifactor Authentication is an extremely important tool which can be used in the fight against successful phishing attempts, due to its nature of requiring more than just a password to prove the identify of who is logging in. As we’ve learned in this class, it’s important for companies to require more than one factor of authentication due to the level of defense it adds for accounts. An attacker would not only have to get a student’s password, but they would also need to have the device the student registered to their account to log in. This would greatly reduce the success of any attacker attempting to gain access to the account, whether it be through phishing, or leaked passwords. In conjunction with MFA, Company X should implement Virtual Private Networks that the students can log into in order reduce the risk of their networks being compromised. Allowing students to access applications and files through a VPN adds another layer of defense which makes it harder for attackers to escalate privileges through the network in the case of a breached account.

When it comes to reducing the success of phishing attacks, Company X should implement some simple Email security policies. One of which being link scanning, which would have any link that is shared inside an email visited through automated bots and checked for malicious intent. This would help cut down on the number of phony links related to Covid-19. As we know, attackers like to use urgency when trying to fool someone, so removing any malicious links relating to Covid-19 would go a long way to protecting accounts. Another email policy that should be implemented is attachment scanning, which would scan any attachments uploaded and sent through email. This would be an automated process and would drastically decrease the likelihood of malware being deployed through email attachments. Since email’s are the easiest way for malware to be introduced to an organization, this is a no brainer for Company X seeing that most students would be receiving hundreds of emails over the course of a school year. Lastly, Company X should implement the email policy of flagging any email that does not come from the Company X domain name as “External”, similar to what WPI does. This automatically helps raise the red flag for students and makes them aware the email they are reading was not sent from someone inside the college. This would help reduce the risk of students falling for fake Covid-19 scam emails since it would clearly show that the email was sent from outside the organization.

I believe if Company X implements both of my security recommendations, they would see dramatic improvement in all areas stated in the question. Defense in layers is the best practice when attempting to reduce the overall success rate of attackers but it doesn’t come without some trade-offs regarding student privacy and security. For instance, in my email policy recommendations, all student emails would be read, attachments scanned, and links scanned. While this does intrude on privacy, I believe the trade-off for the amount of security provided is well worth it seeing that it’s not a person who is doing the reading, and scanning. Since the process is entirely automated, it can be announced to students who join the college that these are things that are in place, which would go a long way to reassuring them that while privacy is a strong focus, the security of Company X and student accounts are held to high standards.

Question 2:



For a medium sized company with a budget of 1000 monetary units, with their biggest threats being phishing campaigns and insider threats, I would recommend the following:

Formal Security Awareness Option – Full Security Plan

Informal Security Awareness Options – Lunch & Learns, Posters

Starting with the formal security awareness options I opted for the full security plan because no matter the size of the company, any money spent on security is money well spent. Although the upfront cost might be high, the amount of money saved on the back end by adverting a potential breach is well worth it for any size organization. Also, since one the biggest threats facing the company is insider threats, the internal auditing that would be done by an independent 3rd party is vital to tampering any chance of an insider threat being fulfilled. Personally, I don’t see how you would run an internal audit inside the company without a 3rd party handling it because the potential insider threat could mask their actions during the auditing stage. Independent audits of the application software could find any changes to internal software by someone in the inside, which could go overlooked if the potential insider was part of the auditing team. This would leave a significant hole in the defense of the organization and weighed heavily on my choice to go with the full security plan. Not only that, but since all software for metrics are provided, it also adds another layer of defense by measuring the impact that the full security plan is having. This would give the company clear information about whether their security plan and awareness programs are working. Since the plan includes 4 trainings per year, I believe that is more than enough to continue keeping cyber security awareness on the minds of all the employees which would hopefully help reduce the potential of phishing attempts being successful.

As for the informal security awareness options, I opted for lunch and learns and posters. I believe that Lunch and Learns have an important role to play because not only does it help boost company morale due to the free nature of the food provided but combining learning with food makes for a memorable experience which is the hope of security training. Memories are strongly formed when all senses are used so combining smells, and tastes along with training will help keep what was learned in the mind of the workers longer than most people think. Though some may see it as a chore to attend, it provides an effective way to keep workers motivated through the year. As far as posters go, if there’s anything that the advertising business has taught us is that subliminal advertising works. Though some people may not even know it, the reason they like a certain brand of drink, car, or restaurant is because they have been conditioned subliminally through the years. There’s a reason why billboards are still an effective way of advertising, and this would have the same affect when it comes to security awareness. Posters could include reminders such as making sure accounts are protected by multi-factor authentication, ways to spot suspicious emails, and steps to take to protect personal identifiable information. Using subliminal programming, employees would become more aware and better equipped to deal with a cyber security incident without even realizing it.

Text

Description automatically generated

Company X in this case is a healthcare company who employees over 15,000 people in Rhode Island. They deal with over 300,000 patients per year which comes with the responsibility of holding medical records in compliance with HIPAA.

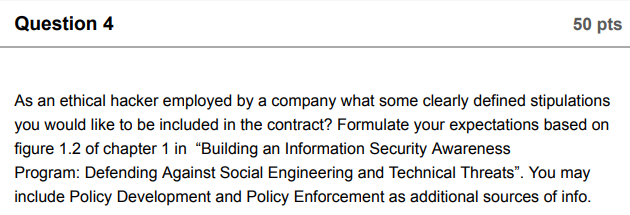
The 3 most significant avenues a malicious actor could use to gather information on my Company X are:

* Online searches to find corporate documents, resumes, floor plans, vendor relationships, phone numbers, job titles, email addresses, and business locations.
* Social Networking Sites which can be used to gather clues and information regarding employee password security questions, find co-workers, and finding what hobbies/interests an employee may have to craft phishing emails.
* Dumpster Diving which could be used to go through the trash to find improperly disposed medical records, resumes, financial documents, and tech support logs

I would address the case of online searches by trying to limit the amount of critical information about the company is put in public searches. For instance, I would require any vendor deals have specific language the prohibit the use of our company name on any publicly accessible website. I would also implement strict policies regarding the use of work email to sign up for any website outside of the organization. This would help limit the amount of information an attacker could use, as well as better protect employees from potential social engineering attacks. I would also advise all employees who used LinkedIn to make their profiles private to hide information such as their job title which could be useful to an attacker in a spear phishing attack.

Regarding social networking sites, I would advise employees to not state their place of work in their public profile, nor take pictures at work and post them to any social network. This would be part of a security awareness program to let them understand why such measures are put in place. This measure would help reduce the risk of an attacker gathering information that could help them bypass password reset questions which could give than access to critical employee accounts. Since people normally post their kids names, hobbies, and interests on social media websites, it makes it easier for an attacker to guess what the answers to their security questions could be. Another measure I would put in place is to not allow the browsing or posting of social media on the company premises. Some social media websites tag the location where the post is made which could also be used to correlate someone’s employment with the building’s location.

Lastly, regarding dumpster diving, I would have a policy in place that shreds all documents after they have been disposed of and removed from locked recycle bins. Due to HIPAA compliance, all medical records that are disposed of are tossed into locked bins. The shredding of the documents would help reduce the chance that someone would be able to piece together critical PII such as names, addresses, and social security numbers that can be found on them. This is one of the biggest measures that can be put in place to help reduce the effectiveness of an attacker doing a dumpster dive. For all documents that are not medical records, such as tech support logs, and financial documents, I would have a policy in place that has them shredded before they enter any open recycle bin.



As an ethical hacker for a company, one of the first stipulations that I would like to be included is a Non-Disclosure Agreement that would state that neither party can talk about the work that was done, or what, if any vulnerabilities would be found. This would protect the company regarding any information being leaked, but it would also help me because in the case of a leak of information, I would be protected knowing that the company violated our terms. This would prevent any litigation from false accusations of leaked information should the company try to litigate the issue in a court of law. Another key stipulation I would like in the contract is what type of protection I would have in the case of my penetration testing leading to network or server failures. While the goal of an ethical hacker is never to do harm to the company, mistakes could be made, and I would want the reassurance from the company that they would not hold me liable should an event like I described occur. Also, I would want clear lines drawn in the contract as to what would be considered abuse of these systems and what is acceptable. This would help set the playing field so to speak as to just how far I could push my tactics to gain access to their networks. Another stipulation I would request in the contract is which employees are off limits to social engineering attacks. Since I would be crafting phishing emails to try and gain access to their networks, I would want to know if certain employees such as the CEO, or any other high-ranking members and departments like payroll or human resources would be off limits since their accounts are vital to the operation of the company. As an ethical hacker, I would first do a physical reconnaissance to gather information which could be useful to me when performing attacks, so some further stipulations I would have would be regarding the physical security. Such as, if I would be held liable for any damages that could occur in my attempt to access unattended ethernet ports on the company premises. Also, I would want it in clear writing that I I would not be held liable for any damaged doors or locks that could be opened using simple tooling such as lock picks.

Lastly, I would have some stipulations regarding just how long I would be able to maintain access to the system if I do indeed breach their security. Since my role is to find any and possibly all vulnerabilities, it would be vital to my operation to maintain access for as long as possible in order to maneuver horizontally within the organization to continue to search for ways to elevate my access to more vital systems. I would also like a stipulation regarding just how much I can do to cover my tracks such as clearing caches and cookies from employees’ computers, modifying and or deleting activity logs, deleting employee phishing emails which I crafted, and uninstalling applications that I may have modified to gain access to their systems. While I would personally retain all of this information for my final report to the company, I would still want to know just how far I could go to make it seem as if I was never there to those who are unaware that I had been hired.