What we did

For this assignment, I chose a local eyewear manufacturer, Wiley X, who allowed me to visit and perform a high-level security audit for school purposes. Since the local site is the HQ, my contact, Antonia, had to ultimately gain approval from her IT team to assist me in the project. In a brief conversation with her colleagues, I explained that the main goal of the audit is to assess their security posture and help ensure they maintain compliance, based on recommendations that I've learned from this cybersecurity course. Considering they're familiar with these types of audits, they were satisfied with my justification and approved the audit.

The objective of this audit was to evaluate the manufacturer's digital and physical security practices, assess any potential vulnerabilities, and develop a plan to address them if needed. By identifying weaknesses in their current strategies, this audit aimed to help prioritize threats, prevent security breaches, protect sensitive data, and mitigate any risks that could negatively impact the business. While this audit is informal and ultimately will not influence their business decisions, the findings were compiled into a report to be reviewed by Antonia. Some of the tasks completed in the audit included examining their physical security (office/sensitive area access), internet connection, supervised computer examination, as well as their backup and recovery processes.

During our initial meeting, we agreed that I'd come on-site, Thursday 11/21/24 at 0800 and work with Antonio to greet and escort me through the building for the entire duration of the audit. The morning of the audit, I arrived at 0800 sharp to begin the process and was greeted by Antonia, who helped me get my visitors badge and approval to move about the building with her assistance. They allotted me two hours to complete the audit, but I was able to complete it in 1.5 hours and within that time I was able to run some light scans on Antonia's computer, get a tour of their data center, and meet some of the IT team and get their input.

After returning from my visit, I reviewed my audit plan to consolidate my findings and provide recommendations. These suggestions aim to help the business enhance its resilience, maintain compliance, and uphold the level of trustworthiness expected of companies operating in today's digital landscape.

What are the results?

Wiley X recently relocated their HQ from California to Frisco, Texas, and with it being a fairly new location, I assumed that they put a lot of thought into planning their security posture and ensuring their practices were up-to-date and best in class. During my audit I learned from the IT team that they perform a scheduled detailed security audit once a year, but often do audits as needed or requested. Compared to the extensive audit they perform annually, my audit plan was very high-level, assessing basic measures such as establishing strong passwords, checking if backup solutions exist, and do they have a plan in place to ensure their data is secure and free of any potential threats that could affect their security posture. Overall, they successfully met all the criteria I laid out in my audit plan, but there were a few things I recommended to strengthen their security plans to ensure they're operating at a high standard and are prepared for any potential threats. My top findings are listed below:

- **Physical Security**

Although this course is primarily focused on the digital security of an organization's practices, the aspect that I found the most interesting, but probably the least considered, is the physical nature of data, devices, etc. and identifying the practices we have in place to protect them from physical harm and theft. So for the visit to Wiley X, I was very focused on their physical posture, and more importantly, how do they verify that the people in the building are ultimately supposed to be there to mitigate those risks. When I arrived to perform the audit, the first thing I noticed is that the main door to the building is HID badge protected and only employees and approved contractors have access. All visitors, including myself must press the call button, be connected to the main receptionist desk, and granted access after verification. Once I arrived at the front desk and was greeted, I learned that another layer of security verification was performed, as I was asked to show a valid government issued ID to be given a guest badge to move about the premises. After scanning my ID and receiving the badge, I had a thought; what would happen if a visitor accidentally took a badge home without returning it, would they then have access to the building? Later in the building tour, I learned that even that small detail was considered in the security processes. The visitor access badge rights are individually assigned based on what someone is visiting for and more specifically, the badge access is granted on-demand, is time scheduled, and do not work for the main entrance.

Even the type of employee you are determines the individual access granted throughout the building, as HID and Biometric scanners are located at almost every entry point to different departments. This includes access to internal offices, manufacturing floors, secure IT locations (ex. Data center), etc. Although assumed, I ultimately learned that they have these measures in place to reduce the amount of unauthorized access that employees and guests have to certain areas and prevent the assessment and/or theft of sensitive hardware, data, etc.

One interesting thing I learned about their badge access throughout the building is that they don't allow shoulder/badge surfing. Each person that walks through a badge protect door, must scan their badge individually, and if not, a motion security alarm will sound until it's scanned and verified.

- **Password strength**

During my conversation with the some of the IT team, I learned that all employees' computers are password protected and must be updated every 60 days. These mandatory password updates are managed at an organizational level and are pushed to the computers 14 days ahead of the password expiration. All passwords are heavily scrutinized and due to security purposes, they couldn't tell me what's all considered, but based on what I learned about password security in this course, I assume it includes: a high number of characters, case sensitive, special characters, etc, to ultimately decrease the likelihood of someone gaining unauthorized access to a machine. All throughout the tour I noticed multiple *brand recognizable* access points, routers, and printers that could easily be compromised with enough research to find their default passwords and later inquired if they change them before they're deployed. I was informed that all internet devices, ranging from employee computers to printers, all go through a rigorous security test before deployed. If a default password exists, the security team ensures that it's changed and is only known by key personnel. I also learned that Mobile Device Management software is deployed on all company issued devices to ensure that high password standards are maintained and can easily be wiped if they were to get into the wrong hands. Also, in the event that an employee doesn't change their password in time to meet the 60-day deadline, the computer is inaccessible until they call the IT help desk and a one-time password can be generated or they have to physically hand it over to them and be verified to change it.

- **Data Center and backup**

The tour of their main data room, which houses all their on-prem and vital hardware devices, was pretty standard from what I've seen at large office buildings. This included extra safety measures that would help their business practices stay up and running in case there was a disaster event, such as backup generators, offloading data to a third-party site, etc. Staying true to their strict security nature, the data room is only accessible via badge access by approved personnel or by using a physical key because unauthorized access with mal intent could be catastrophic if a successful attempt was made. I learned that they have a backup generator that can last for a few days in case of an electric outage to keep their network running and to allow vital business processes to continue. The generator also supports their security measures such as the alarm, cameras, etc. Also pretty standard in most established business sites, the data room also has a separate HVAC system from the rest of the business and powered by the generator in case of an electrical outage and is always set at a constant temperature. Considering that summer temperatures reach well over 100 degrees, in the event of an electrical outage, it wouldn't take long for the building's temperature to reach levels that can potentially damage their most important assets. I was also quite impressed by how neat all the devices and cables were kept, dramatically reducing the event that someone could have an accident and disconnect it from something important.

- **Employee computer assessment (updates and malware protection)**

In this course I learned that keeping devices up-to-date is one of the easiest ways mitigate the increased exposure to security breaches. Because some hackers prey on

vulnerabilities within out of compliance devices and exploit it for some sort of gain. So ensure that all employees maintain security compliance on their computers, I learned that the IT team also remotely pushes out update requests and gives employees up to 30 days to meet the compliance. The result of not updating a device to meet the IT criteria within the 30-day deadline, means that a user will not be able to access their device. This also seems to be pretty standard within most established and tech savvy businesses today because my current company does this as well. I learned that the automatic software update toggle button on the machines is statically set to off before deployed and that all updates are vetted before they're pushed out by security.

Through a supervised examination of one of the company issued computers, I was shocked to not see any visible malware protection on the machine and when I asked if it even exists, I was told that they couldn't answer due to security purposes. Given that they have stringent security measures in other parts of their business, I assume they deploy malware protection. Based on what I know about the customizable nature of today's computers and from one of the keylogging exercises we performed this semester, I understand how easy it is to make something visible/invisible to an end user and they'd never know the difference.

- **Internet access**

One thing I thought was pretty interesting in an effort to maintain a great security posture is that they don't outright let guests/visitors connect to their guest Wi-Fi network unless verified by another employee. This also excludes having a static password for the guest network. For instance, when I wanted internet access in the main conference room and tried to connect to the guest network, I was redirected to a splash page that prompted me to enter a valid employee's email address. Once the email address was verified, it then sent a link to the employee to further verify my existence, which could then be approved remotely. In a stricter effort to maintain their security posture, even after being verified by a valid employee, the guest access is timed and automatically disconnected after an hour. I followed up with the IT team about this measure and they mentioned that although very important, it's not so much of a security concern as much as it is a bandwidth concern. I also learned that without certain restrictions, guest users may consume excessive bandwidth, slowing down their internet connection and disrupting business-critical operations.

What are the recommendations

After pinpointing the top five findings from my audit, I am providing the following recommendations on how to address them in a cost-effective manner while minimizing disruptions to business operations:

- **Physical security**

Based on what I learned about the physical security measures to keep the employees, devices, and data safe, it's my conclusion that Wiley X has great systems in place to mitigate unauthorized access. Especially with their visitor access and registration process and the shoulder surfing mitigation strategies. The only recommendation I'd make here is that I noticed that some of the cameras on less secure areas, for whatever reason, were simple battery-operated Blink branded cameras. This differed greatly from the more high-tech cameras that are hardwired around highly secured areas. The concern here is that if there were a disaster event or if they lost electricity, these devices wouldn't have the same mitigation plans regarding if they can be powered by a backup generator. I assume someone must've considered this risk and used some version of the risk formula we used in previous assignments and determined that the risk wasn't worth going through the trouble of hardwiring the less secure cameras. Hardwired cameras usually cost roughly between $250-$1000 and take less than an hour to hardwire.

- **Password strength**

Although impressed that they have strict measure in place to ensure that employees update their passwords every 60-days, depending on how severe a password cracking risk is, I think that every 60 days can be a bit excessive. Mainly because after further conversations with the IT team, the confirmed that they're often inundated with password reset requests and that it can sometimes take them away from other important tasks. In fact, cybersecurity experts only recommend that you change your password every 3-6 months and can still be in compliance, but I assume that the 60-day rule is coming from the top of the organization. One recommendation that they could do to reduce the number of calls/tickets they receive to reset passwords is to implement a daily email notification workflow to ensure that the employees receive the message in two forms of communication and can reset their passwords accordingly. I assume they can use one of their existing customer email marketing tools and can also point messages to their employees, but the real cost would be the IT man hours to implement the system and tie it in with their updates. Alternatively, they could use an implementation partner who'd charge approximately $5K-20K to complete the job and would need at least a week max.

- **Data center and backup**

During my audit of two of the data rooms, I noticed that the smaller of the two was located on the first level. The office location isn't prone to flooding but in the event of a flooding disaster, depending on how bad, the vital components of the lower-level data center could be affected. My only recommendation here would be to consider moving it up to the second floor with the larger data room. As noted above, I assume someone considered this risk when planning for this new location and considered that the risk isn't high enough to mitigate if a disaster event were to take place. All things fair, I didn't inquire much about the second data room after seeing the first one, so I'm not sure vital the assets are on the lower level. If they were to consider moving the smaller data room to the upper level, since they already have the equipment, my assumption is the mitigation strategy would be a low financial cost and consume a few man hours to

physically move the equipment. The only other thing to consider is if the upper level can even house the assets and offer enough networking connections to support the additional equipment.

- **Employee computer assessment**

Wiley X already has a good practice in place when it comes to how they manage and secure their company owned devices, especially with the push notifications to update the devices and how they deploy Mobile Device Management software to ensure compliance. This is nitpicking but one thing I noticed that could strengthen their security posture is to not allow certain external devices to connect to their company computers. For instance, at my current company, employees cannot connect external hard drives or thumb drives to the company computers. When attempted, you're prompted with a notification that says there are security measures in place that won't allow it. Therefore, all sensitive documents must be stored in the cloud. Based on that I know about personal storage options, it only costs about $10 a month for 2TB of data within Apple iCloud for personal use. I assume that a business would receive a much larger volume discount, and they most likely already use some form of cloud storage that they could offload that task to and reduce the risk of misappropriation of data.

- **Internet access**

I was quite impressed at the level of security they imposed with their guest internet access, given the fact that all guests must be verified by a valid employee to complete the connection process. But during my assessment after visiting the business, I wondered what would happen if their employee notification system failed and they could no longer grant guest access in the intended way? How long would it take to fix? Although very minor, my recommendation would be to have a readily available backup password or establish a temporary password process, similar to their visitor badge access, so that guest can establish a connection in case there was a failure event.

What is the risk posture

Based on the plan I created for the audit, I believe Wiley X passed and their risk posture for potential threats is very low, mainly because I feel that a lot of thought has gone into their planning process and that all bases were covered when they established their new HQ location. The organization has several systems designed to maintain business continuity in the event of power or network failures, as well as robust security measures to prevent unauthorized access to systems containing sensitive business and customer data. Based on my evaluation, I believe they've done an excellent job safeguarding their network from external threats by implementing straightforward but effective solutions, such as automatic updates, strict badge access protocols, and mobile device management software. However, I feel their most significant vulnerabilities are internal and could be addressed with a few minor adjustments.

Considering that the threats I mentioned earlier are primarily internal, I believe they can be resolved relatively easily. Based on my evaluation, the company appears well-protected against external threats, as their IT team has effectively implemented systems to mitigate these risks and maintain strong security measures. From what I was able to assess in my short visit, their greatest risk was the allowing of external storage devices to be connected to their employee devices. To be fair, I believe the thumb drive that was used during the demonstration was company issued, but even then, that's just one extra piece of hardware that can be exploited if it were to get in the wrong hands. I assume that a non-company issued piece of hardware would not be able to successfully make a connection.

Based on further research, I found that a low-risk posture is generally favorable when security, compliance, and operational stability are critical. However, it's important to balance caution with flexibility to avoid stifling progress or innovation. For most organizations, the key is to assess risk appropriately and implement a risk posture that aligns with their overall objectives and risk tolerance.

Audit Plan for Wiley X

Purpose

The purpose of this audit is to assess Wiley X's overall security posture (physical and digital), identify vulnerabilities, and ensure compliance with relevant IT regulations for the manufacturing industry. Additionally, the goal is to assess the company's attack surface and establish a plan to mitigate in the event of a breach, internally and externally.

Outcome

The outcome of this audit will be recommendations for the Operations Manager of Wiley X and share them with the appropriate leadership in the IT/Security department for review.

Scope

The scope of the audit will be to review the physical security, internet connection, review existing security plans, and data processes in the establishment.

Audit Procedure

Arrival: The auditor will arrive at the headquarters (15755 Preston Rd, Frisco, Texas 75033) and contact the Operations Manager (Antonia Mo'Ne) to register the auditor as a visitor to grant permission to move about the premises. The auditor will then be escorted by Antonia to inspect the areas listed in the Item and Observations sheet attached to this plan.

Introduction: Once the auditor is satisfied with the visitor registration process, they will introduce themselves to Antonia Mo'Ne to begin the audit exercise.

Audit Meeting: After the introduction, the auditor will be escorted by Antonia and introduced to any key stakeholders, if necessary, to complete the attached audit plan documentation. Items may be added to the audit plan as needed and as agreed between the auditor and Antonia. Any items added while performing the audit exercise will be documented in the blank spaces attached in the audit plan.

Audit Hot Wash: After the audit plan document is completed, the auditor will review it with Antonia and schedule a follow-up meeting to make recommendations. The purpose of this meeting will be for the auditor to review the preliminary findings and work with Antonia to agree on any needed action items to strengthen their overall security posture.

Audit Commenced (time/date): 0800 11/21/24 **Audit Complete (time/date):** 0950 11/21/24

Auditor: Danzel Barber

Antonia Mo'Ne, Operations Manager:

	Audit Plan: **Items and Observations** **Auditor: Danzel Barber**		**Date: 11/21/2025**	
Item #	**Description**	**Expected Findings/pass criteria**	**Observations**	**Pass (Yes/No)**
1	Review visitor/guest check-in process	Receptionist performing credential checking for all guests	Rigorous registration process	**Yes**
2	Check password strength	Should be strong: no dictionary word or easily recognizable repeated characters	Passwords are strong with updates required every 60 days	Yes
3	Check ports using shield's up	Ports are in stealth or at least closed	IT would not approve this item	N/A
4	Check for missing updates	Computer is up to date with auto updates on	Assessed employee computer up-to-date	Yes
5	Check for back up	Back up exists	Business has cloud storage available for backups	Yes
6	Computer is kept in a location with controlled access	Access is limited to those with a need	Computers are issued to all employees. MDM software deployed	Yes
7	Review computer files for possible malware	No malware found	Security scans are maintained by IT	Yes
8	Check for access control on personal files	Only computer owner can access all files	Heavily password protected by employees only	Yes
9	Check for malware protections	Malware protection active	Protections exist, but not visible to end user	Yes
10	Check for surge protection on power supply	Surge protection present	Data center and desk locations have individual power strips	Yes
11	Check Router in location with good air flow	Air flow and temperature okay	Data center is climate controlled	Yes
12	Router is kept in a location with controlled access	Access is limited to those with a need	Only accessible by badge and key access by key personnel	Yes
13	Ensure router is password protected	Password is active	Only accessible by IT team and key personnel	Yes

14	Ensure access controlled on all business systems	Access is controlled	Access is given and maintained by key personnel	Yes
15	Ask about a security plan and review if an existing plan is established	Security policies are in place	Security mitigation plans exist in case of an emergency	Yes
16	Check for other digital devices	No other devices	All digital devices are accounted for with IT inventory	Yes
17	If additional devices discovered check for the above on them	Passwords, backups, access control exist	Policies are in place and managed by IT team and key personnel	Yes
18	Checking for training and recovery plans	Training plans around awareness, phishing, business email compromise ransomware plan	Training and mitigation plans exist in case of an emergency	Yes
19	Checking for security cameras and secure connection	No default passwords	All devices are vetted by IT security for default passwords before deployment	Yes