Information Security Management
Organizational Analysis and Recommendations

Office of Graduate Admissions, Worcester Polytechnic Institute

Point of Contact: Paige Dunn, Senior Assistant Director
Team 4: Brian McKay, Kushal Shah, Nnenna Jennifer Ajuzieogu

Table of Contents

Executive Summary

The Office of Graduate Admissions has been thoroughly analyzed to properly identify its information systems, networks, data stores, and processes. Through this analysis, some vulnerabilities may pose a potential threat to the information security within this organization and also allows the identification of unusual threats that might be present in the future. The Office of Graduate Admissions uses Slate as their constituent relationship management (CRM) software and is the primary application and operating system that all the staff use for daily operations. Acxiom is also used as their primary data management platform (DMP) software which allows the transfer of student data from Slate to WPI's BannerWEB. A transition to remote work has also brought new challenges to the security posture of this organization. Identification of vulnerabilities has been examined in many areas of a strong information security posture which include identification and authentication, authorization and access control, auditing and accountability, operations security, physical security, network security, and application and operating system security.

After careful analysis, there are evident weaknesses in many areas of a strong information security posture. Authentication within Slate is vulnerable due to a lack of strongly enforced password rules when authenticating into the application. In an instance of a possible cyberattack on the application, a lack of a contingency plan within the department has weakened the director's ability to respond and ultimately rely on the IT department to maintain their availability to it. There is also a lack of an auditing plan within the department, which weakens any accountability of actions of all staff that uses Slate. Slate has also acknowledged potential security issues which cannot be dealt with by them such as clickjacking, DoS, policy issues, etc. Acxiom has also been proved to be vulnerable and has been the victim of a security breach in 2003. These bring a lot of potential attack vectors and demand strength in other areas. The pandemic has also brought additional weaknesses to this organization. Physically maintaining the safety of the staff within their private working environment is a challenging task, as the staff is ultimately responsible for their safety. The analysis of the physical protection of data has yielded a high measure of availability to users however, there are weaknesses with how much of this data is available. In terms of protecting computer equipment, staff do use college-owned devices however, there are usages of personal devices that can bring additional attack vectors. This use of personal equipment potentially connecting to the VPN can cause a weakness in the network as security restrictions are not applied and can be a gateway for malicious activity. Another gateway for malicious activity could be potential phishing campaigns through email. Although this is a known threat throughout the Office of Graduate Admissions, there is no current security awareness program in place, which neglects the evolution of these types of attacks.

The weaknesses that the Office of Graduate Admissions contains demand a stronger information security plan. Although encryption is strongly implemented within the operational resources of this organization, these vulnerabilities open up other attack vectors which render this strength useless. Defense in layers will make this organization stronger and more ready for any potential cyber attack. These layered defenses come in the form of all the areas of a strong information security posture and will accurately maintain the confidentiality, integrity, and availability of the data and information systems within the Office of Graduate Admissions. Thus, it is strongly recommended that the Office of Graduate Admissions considers the recommendations in order to mitigate these analyzed weaknesses.

Organization Introduction

Worcester Polytechnic Institute (WPI) is a private institution that was founded in 1865. The location of the school is Worcester, MA. This analysis focuses on the department of graduate admissions at WPI and its existing information systems, processes, networks, and data stores. The department guides future students with the graduate admissions process and academic programs. They also assist students in accomplishing their professional degree goals. There are about ten employees in the department. The senior assistant director at the department, Paige Dunn, has been assigned to provide us with any information we may need to complete this analysis. The project would analyze every area of information system security and provide analysis of vulnerabilities in these areas. From this analysis, recommendations will be given in order to mitigate these vulnerabilities.

Conduction of Analysis

The organizational analysis was conducted over two meetings via Zoom. During the first meeting, Paige Dunn (Senior Assistant Director) and Melissa Terrio (Executive director of grad recruitment) agreed to answer questions pertaining to each area of information security. This meeting was longer than the first, and emphasized each area in order to sufficiently analyze the current security posture of the Office of Graduate Admissions. Then, based on the information and through further analysis, Paige Dunn agreed to meet with us for a second meeting in order to answer more specific questions that needed clarification. Each team member was assigned specific areas of information security pertaining to this organization. This allowed a more in-depth analysis on each area, and accurately depicted the current security posture of this organization. This analysis of their security posture yielded weaknesses in many areas.

Supervisory Acknowledgments

Nnenna Jennifer Ajuzieogu served as the primary contact between the organization and the group members. She made all contact with Paige Dunn via email and scheduled all Zoom meetings between both parties. Jennifer was responsible for three components of information security management which are identification & authentication, authorization & access control, and auditing & accountability. Brian Mckay scheduled weekly group meetings with the group members and assigned individual tasks throughout each process of the analysis and recommendations stage. He also made sure assignments were completed by certain dates and communicated goals effectively. Brian was responsible for analysing cryptography, physical security, and the development plans for a comprehensive security awareness program. Kushal Shah was responsible for analyzing network security, operation security, and application/operating system security. Each person assigned to their respective area of information security was also responsible for contributing that portion to this analysis report which includes analyzed vulnerabilities and recommendations to mitigate these weaknesses.

Organization Analysis and Vulnerabilities

Identification and Authentication

Identification is simply an assertion of who we are. It comprises a naming system that an employee is given and must comply with to gain access. It can either be a username, ID number, or both. In the office of graduate admissions, staff and faculty members that need to access a student's application get their user account for Slate.

Authentication is a cybersecurity technique that establishes a claim of an identity as being true. Staff and faculty members use their WPI username and password to access Slate. A VPN is used to connect to the school resources through this means. Since it is synced with each user's WPI account, two-factor authentication is activated.

Vulnerabilities: The information technology department is in charge of creating WPI accounts for all faculty members and students in the school. One vulnerability could be enforcing password rules to slate. Users should not use weak passwords and recycled passwords. Strong passwords should include the password length, require a mix of letters, numbers and function keys, password history, and password expiration. Passwords should have an expiration date, this would help remind account owners to frequently change their passwords. Slate also has an indefinite login time which could lead to security risks.

Authorization and Access Control

Authorization controls the degree of access and the capacity to change, alter, or spread sensitive data. In the department, Paige Dunn who is the senior assistant director gives and revokes privileges on Slate. For instance, a faculty member within a department needs to verify classes on a transfer student's transcript, Paige would grant them access to Slate.

Access Control is a security measure used to minimize unauthorized access to the physical and logical systems. Access control focuses on four basic tasks; allowing access, denying access, limiting access, and revoking access. Only faculty members that are in charge of admissions within their department can access Slate. With Slate, the principle of least privilege is used in that faculty members have access to only their department applications. Limiting access within each department would prevent applicant's information from being compromised. Slate uses a mandatory access control model, the initiators at Slate do not get to decide who gets to access it, but access is decided by the information technology and graduate admission at WPI. The end-user has no right or control over any privileges.

Vulnerabilities: Because the IT department does more of the technology-related work with Slate, Paige can only manage Slate to an extent. In the case of a cyberattack, there is no contingency plan within the department of graduate admissions. There are no measures that have prepared Paige for such an event. Therefore, only the IT department would be able to solve such a problem. Paige should have a control measure to assist from her end in case of an emergency.

Auditing and Accountability

Accountability enables us to trace activities in our system/environment back to their source. In case of a situation, accountability can know who the transaction was associated with and what permissions were used to allow them to carry it out. The information technology department at WPI monitors all software (Slate and Axiom) that the office of graduate admission uses. When a situation arises, they know who to hold accountable.

Auditing helps to test and assess the organization's overall security posture. It would ensure that all users and administrators are adhering to the security policies. Auditing is an effective way for ensuring accountability. Slate is appropriately licensed, and the IT department verifies that from time to time. Paige audits account privileges once a year, based on who she is aware has left or is leaving the department and WPI. She mentioned that the yearly auditing needs to be more organized in the future. Once an employee leaves WPI, IT will revoke their WPI account, which would automatically remove the user's privilege from Slate.

Vulnerabilities: The lack of an auditing plan within the department is a vulnerability. Last year, the Slate controller retired, and Paige was given the fastest training possible before he left. A detailed and less complex audit plan that pays attention to all security policies in Slate would make the process straightforward. A training video that emphasizes Slate security policies should be made available to all staff members. It will serve as a reminder that everyone must obey all laws and policies while using Slate.

Cryptography

The integration of cryptography is important in order to keep the information within the Office of Graduate Admissions secure. The confidentiality and integrity of the data within this organization is reliant on the encryption from three important sources. These sources are examined in the encryption methods of Slate, Acxiom, and through the use of a Virtual Private Network (VPN) when accessing resources remotely.

Slate Encryption: The main goals for the encryption of the data within Slate is to protect both sensitive data at rest and in motion. Sensitive data is at rest, or stored, in a database; whereas data in motion is when Slate collects data from applicants. Protection of data in use is not considered as it is reliant on proper access control by authorized users of Slate.

Slate is used to store sensitive documentation such as a student's transcripts, financial records, and other personally identifiable information (PII). This information at rest should be properly encrypted to protect the confidentiality of this data. The confidentiality is considered for the data at rest, as it must be encrypted to prevent unauthorized access. As per the Slate "Security and Privacy" policies, Slate uses industry-recognized security safeguards such as firewalls, coupled with carefully developed security procedures to protect the data from loss, misuse, or unauthorized alteration.

The integrity of the data within Slate must be considered during collection and transmission to Slate. Integrity of this data is considered to prevent deletion or modification from any unauthorized party. When Slate collects sensitive PII, the transmission of this data is protected using Secure Socket Layer (SSL) protocol encryption. Although the application itself is using

SSL to protect the data in motion, it does not mean the connection made through the Web Browser has the same level of increased security. This is considered through the use of a VPN. Acxiom is used to transfer this data from Slate to BannerWEB.

Acxiom Encryption: The main goal for the encryption of managed data from Acxiom is to protect sensitive data in motion from Slate to BannerWEB. Acxiom is used as a loader for application data between Slate and BannerWEB and is also used to upload transcripts and other sensitive documents.

Acxiom automatically applies protection as data moves. This makes the transmission privacy-compliant by properly applying encryption. Acxiom's data centers and operations are System and Organization Controls (SOC2) certified and meet all requirements for handling the data from Slate. This ensures both the confidentiality and integrity of the data in motion from Slate to BannerWEB.

Encryption for Accessing Resources: The main goal for staff accessing resources remotely is to encrypt each session by using a VPN. Currently, operations by the Office of Graduate Admissions are completely remote. In order to encrypt each individuals' access to operational resources, a VPN connection is used which utilizes encryption using IPSec. This ensures the confidentiality and integrity the resources staff are utilizing, and also adds an extra layer of security in addition to the encryption methods by each resource.

Vulnerabilities: We believe proper encryption methods have been utilized in all important operational areas of the Office of Graduate Admissions. Each user's web experience is properly encrypted through the use of WPI's VPN when accessing resources. Additionally, methods of encrypting data within Slate and Acxiom are properly utilized and ensure both the confidentiality and integrity of the data from all applicants of WPI. With these layers of encryption, we believe there are no immediate vulnerabilities in the area of cryptography.

Operations Security

Operations security is often referred to as OPSEC. It not only means putting countermeasures in place, but it also specifies an understanding and identifying what data we need to protect. WPI makes use of Slate and its privacy policies for Operations security.

Slate has acknowledged some security issues within their software. Acxiom has also been proven to be vulnerable and has been hacked once before in 2003.

Vulnerabilities: The following items are known issues or accepted risks and are out of scope for Slate:

Clickjacking: Clickjacking, also known as a "UI redress attack" is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were expecting to click on the top-level page. It means that when a person intends to click on something on the slate webpage, he might be clicking on a page below. It can be used for a variety of things, including permitting cookies or a download button which would, in turn, affect the given system.

Missing additional security controls, such as HSTS or CSP headers: Modern websites are a complex mix of content, resources, and JavaScript that creates a rich, dynamic user experience. All of this content is loaded and executed by the browser on the user's computer or mobile device, which improves performance and responsiveness. However, this also creates an attack surface for hackers to inject and execute malicious scripts from alternate domains. These scripts can be used to execute cross-site scripting (XSS) attacks or digital skimming attacks such as Magecart that result in the theft of personal data from the website. Content security policy (CSP) is a useful tool in the fight against unauthorized Shadow Code that plagues web applications. The lack of CSP or HSTS headers means that the slate website can be subject to the above attacks, making the data on the website vulnerable.

Brute-force, Rate-limiting, Velocity throttling, and other denials of service-based issues: Rate limiting is a strategy for limiting network traffic. It puts a cap on how often someone can repeat an action within a certain timeframe; for instance, trying to log in to an account. A Brute-force attack is a trial and error method used by hackers to guess credentials or encrypted data such as login, passwords, or encryption keys, through the exhaustive effort with the hope of eventually guessing correctly. The brute-force attack is one of the most popular password cracking methods for hacking WordPress. A Denial-of-Service (DoS) attack is an attack meant to shut down a website or a web server, making it inaccessible to its intended users by flooding it with useless traffic from a single host. It means DoS attacks can be used for destroying computer defense systems meant to keep Slate online. It then makes the WPI data within Slate vulnerable.

Physical Security

Physical security is largely concerned with the protection of people, data, and equipment in that specific order. The biggest challenge in terms of physical security is that the Office of Graduate Admissions is working fully remote due to the pandemic. This means there are no logs of physical equipment being used by staff, and the activity they pursue on their workstations is not limited as each person is working privately from home. These issues bring along unknown variables that are more challenging to secure.

Protection of People: Physically protecting the people of this organization is an impossible task, as we do not know the physical environment in which each person works remotely. Therefore, the people working in their own physical environment are responsible for their own safety.

Protection of Data: Physically protecting data is less of an issue in regards to a remote environment where availability of this data is a major concern. The data within Slate must be available to the staff of Office of Graduate Admissions and other users of Slate. Since Slate is offered as a SaaS and runs in the Amazon Web Services cloud, the data is stored off-site from the college campus. Slate utilizes a multi-availability zone and multi-region deployment for high availability and disaster recovery, and maintains backup of data. Each institution that licenses Slate is housed within its own private database, and is never commingled with other data. As per Slate, there is 99.999% typical availability, amounting to less than 5 minutes of total downtime, including scheduled maintenance, during a calendar year. Although there is strong availability of this data, there is a concern with residual data. Throughout its historical use at WPI, student application data has never been deleted and remains in the database to be viewed at any given time. There are also no enforced policies within the department that require the regular review and deleting for data that is no longer needed.

Protection of Equipment: A major aspect of availability relies on each user's equipment to work properly at all times. Physically protecting equipment that staff from the Office of Graduate Admissions utilizes is also a challenge given the current remote environment. The department does utilize college-owned equipment such as laptops, desktops, printers, or other equipment needed to operate normally. There are unknown variables, however, which might include additional equipment from staff that is unknown and the physical conditions in which the equipment is located. There are also no current logs of which staff has what equipment. These factors are concerning, considering without proper protection of equipment, there is no feasible way to operate normally.

Vulnerabilities: The remote environment has brought more challenges in terms of physical security at the Office of Graduate Admissions. Protection of staff, which is the most important physical protection to consider, brings a lot of concern to the private environment in which staff are working and how they are properly protecting themselves. In terms of data, there is a very high measure of availability, but there is also a lot of residual data within Slate that is not actively monitored or deleted which contains many applicants' PII. The data must be rendered inaccessible when it is no longer needed. Finally, in terms of equipment, although staff are using college-owned devices, there are no logs of how the devices are distributed or used, if there are other non-college owned devices being used, and the means in which the staff are physically protecting their equipment are unknown.

Network Security

There are plenty of vulnerabilities present in network security. Attacks on network security aren't the only problems it can be due to simple misconfigurations or loss of power. Network security can be in many forms, for example, by network designing and arranging layers in a way that makes it more secure. We can also install devices within the network like firewalls to help prevent things like DDoS attacks. WPI has taken to using their VPN server for work from home in the step of network security.

Vulnerabilities: Employees use their own devices during the covid WFH policy. The devices access the network firewall from their devices meaning, they may not have the necessary security in place. The VPN could avoid the risks of network, but the issues like updated software, licensed products, trojan horses. It means that even if one system is compromised, it allows the hackers to gain access to the whole VPN network by piggybacking on that one system. The employees were asked to take home devices from the office, meaning they have certain software and application restrictions, that also means that the office devices could be corrupted using a simple phishing mail if the employee is unaware which in turn would compromise the entire network.

Operating System and Application Security

Operating systems are one of the largest areas to find vulnerabilities. We can add tools and systems to protect the operating systems as, without securing them, we do not have a foothold in security systems. Several software issues can compromise application security. WPI makes use of the application and OS of Slate to have a relatively secure base.

Vulnerabilities: Slate has a policy that states that personal Information once de-identified is not subject to Slate's privacy policy listed here: https://slate.com/privacy and may treat it as non-Personal Information and use it without obligation to the users except as prohibited by applicable law. Also, Slate does not clear cookies or cache regularly. Student data on Slate is never cleared, including the rejected applications or those with an incomplete application. The student data that is never cleared has no operational use and can cause a major privacy risk.

Development Plans for a Comprehensive Security Awareness Program

Social engineering and phishing campaigns are active threats to any organization. A strong security awareness program is necessary in order to modify the behavior of staff within the Office of Graduate Admissions in the direction of being more secure.

The department staff is knowledgeable of the threats of phishing campaigns and other typical security threats. As new users are added to Slate, or a department has a new graduate coordinator that needs to review student applications, Slate training is offered by Paige. During this training, student privacy is emphasized and is compliant with federal privacy laws. Staff within the office of Graduate Admissions does not disclose application status to anyone other than the applicant.

Security awareness and education is given to the staff as they are hired. As an example, Paige was hired at WPI in 2017 and received security training on the basics of phishing threats and social engineering. However, she has not received any training since she was hired. The details of how this training was distributed was vague, and it does not seem to be a regular concern within the department.

Some risks faced by the organization include reconnaissance through search engines such as Google. A quick Google search using a query such as "Company name" sensitive file type: Xls gives an idea of the documents that the organization has on their website and what kind of sensitive and private file types they have. The search results are mostly from web.wpi.edu and they contain the projects and various details regarding what kind of projects and the students who performed the projects thus giving the information-gathering part of social engineering easy. This can be dealt with by making the web.wpi.edu page strictly for the WPI id, and those who do not have a WPI id can not access to download or view the files on the website.

Another threat is by also using social media to gather information about employees at the Office of Graduate Admissions. One way an attacker can gather information about an employee is through their social media account. An attacker can collect information about their target through LinkedIn, Facebook, Instagram e.t.c. It can be difficult to encourage employees to avoid sharing sensitive information on social media. Providing scenarios while raising security awareness on what WPI deems unacceptable to share and how the information can be used to target the department is a good starting point.

Finally, a very common social engineering risk is that of email phishing campaigns and/or phone phishing AKA vishing. The office of graduate admissions uses email and routed phone calls to their remote environment to complete tasks daily. Especially in the current remote environment, attackers are using more sophisticated means of social engineering to trick users into entering personal information or credentials through phishing or even impersonating other staff members or IT through spoofing phone calls. To reduce this risk, staff needs to be trained on indicators of phishing/vishing and understand the current threat environment by receiving yearly training.

Vulnerabilities: Although the staff is knowledgeable of the typical threats one would be educated on during training, there does not seem to be any comprehensive security awareness program in place. This is cause for major concern considering that there is no regular training of how to spot indicators of phishing emails or a social engineering attempt. These types of attack techniques are always evolving, especially due to the transition to a complete remote work environment.

Recommendations to Improve Information Security Management

Through analysis of the Office of Graduate Admissions and the discovery of many vulnerabilities within most areas of Information Security, the following recommendations are strongly advised and should be considered in order to protect the confidentiality, integrity, and availability of the organization's information systems and processes.

Identification and Authentication

Implementing a password policy to all WPI user accounts would minimize the risk of a security breach. Enforce password history so that there would not be repetitions. Each time a user changes their password, it should be new, and it cannot be a word in the dictionary. All passwords should be unique, randomly generated, and consist of at least eight characters. All eight characters or more should include lowercase and uppercase alphabets, numbers, and symbols. Setting a maximum password age can help users remember to change it often. Passwords should expire between 60 or 90 days to help ensure network security.

Slate should have a limited login time and "remember me" features. Users should not remain logged in after 8 hours. Slate should automatically log out users after 8 hours, and request for a password to gain access. There should be a limit of devices that a user can be signed into when using Slate.

Authorization and Access Control

In creating a contingency plan, the first step is to conduct a risk analysis by identifying all types of potential risks within Slate. Analyzing the consequences of these risks would help to create an effective plan for the department. After the risk analysis is completed, the risks should be prioritized by the level of importance. It is necessary to have different ways of dealing with all types of scenarios and step-by-step procedures to mitigate each risk. Communicating with the IT department would also help in creating an in-depth contingency plan. Once all aspects are considered, the contingency plan can be developed. Regularly, the plan must be revisited, revised, and maintained to reflect the changes made within Slate.

Auditing and Accountability

An audit plan is necessary to be certain that Slate is functioning correctly, meeting standard criteria, and appropriately licensed. It should focus on the department's daily use of Slate to achieve its objectives and strategies. The plan must consider the efficiency, effectiveness, and compliance of Slate. It should also include preliminary checks that update all information within Slate, a risk review, security policies, and process coordination. Mapping out the system and data flow should be included in the audit plan. It would provide a thorough understanding between Slate and other applications, the process, the controls, and how they fit together. Once all this information is collected, Paige can create a comprehensive and straightforward plan. Providing Slate users with a short video or pamphlet that reminds them about its security policies would keep them on their toes to obey the rules.

Cryptography

Although there was a strong implementation of cryptographic processes within the processing of information and use of resources, it is not something to be neglectful or overly confident about. Cryptographic algorithms can be cracked, and even if the current implementations used by the VPN, Slate, or Acxiom are secure to today's standards, these might not be as secure in the future. Due to this, it is important to regularly monitor the cryptographic algorithms and processes that are implemented within these applications. When using third-party software to handle sensitive data such as the information within the Office of Graduate Admissions, the customer is reliant on the provider of the software to maintain current security standards, and implementations of cryptographic algorithms are a major part of this process. As long as the software is still supported by its vendor, it will regularly receive security patches and updates. To keep the most secure algorithms, it is important to actively apply these updates and patches as soon as they are rolled out.

Operations Security

Clickjacking attacks wrap a page the user trusts in an iframe, then render invisible elements on top of the frame. It can be avoided by making sure the website and the browser directly take in instructions using the HTTP headers or by using client-side java headers (on older versions). The office can use a content security policy to allow the whitelisting of individual domains which can allow scripts and fonts to be loaded and also limit the number of domains that can embed the pages.

SPF is a DNS TXT record that specifies which IP addresses and/or servers are allowed to send email "from" that particular domain. Just like an SPF record, DKIM is a TXT record that's added to a domain's DNS. And if SPF is like a return address on a letter, DKIM is like sending that letter via Certified Mail as it further builds trust between the sending server and receiving server DMARC is an acronym for "Domain-based Message Authentication, Reporting, and Conformance". It's an email authentication, policy, and reporting protocol that's built around both SPF and DKIM. DMARC verifies if the sender has both SPF and DKIM. It also tells the servers what to do if the sender does not have them. Since Slate does not have safety in place, the office should work to ensure that they have these three protocols in place to avoid security threats like phishing and bugs via emails.

The HSTS and CSP securities will allow the office to ensure the employees browsing history are secure. The CSP policy if implemented will ensure that the users who visit HTTP sites behave like the HTTPS sites and the HSTS stands for The HTTP Strict-Transport-Security. This tells the browser that the website should only be visited HTTPS and not HTTP thus, ensuring that the users do not use any unsecured sites.

The most common solution for brute-forcing is Blocking after a certain number of attempts, but locking out could lead to DDoS attacks and cripple the system. Another solution the company can use is slowing the password entry, making it harder for brute-forcing and effective against a single brute force link. The office can work on blocking IP addresses with multiple failed passwords instead of locking out the account. Another solution the office can use is to give out different error messages each time an incorrect passiu8u8word is entered. It makes sure that automated systems can not brute force their way through. A captcha can be used for the same purpose. Velocity throttling and other DoS attempts like Rate limiting can be prevented if the office makes sure to properly allocate their resources and uses resource management allocation to prevent the resources all being sacrificed in a single DoS attack.

Physical Security

Although it is a challenge to physically protect each employee given their remote work environment, usually at home, there are several best practices the employees should take to maintain their physical safety and the protection of college-owned devices and their data. These best practices can come in the form of work-from-home or remote-work security policies and can be further enforced with a comprehensive security awareness program adapted to the increasing remote environment. Also, several administrative controls are necessary to further protect college-owned devices and their data.

Since employees are using college-owned laptops or computers, there is sensitive data on these devices. Employees should always lock their doors to ensure that their device is not stolen in case of an attempted robbery. This will prevent the loss of sensitive student PII, which if stolen, will harm the college in terms of reputation and deterministic fines depending on the amount of data stolen. If the device is a laptop, it is important to only keep the device at the employee's home and not to bring it with them anywhere besides that. This runs the risks of it being stolen out of the employee's vehicle or in a public place and is potentially harmful if connecting to a public unsecured Wi-Fi connection. To further protect these devices and their data, peripheral storage devices should never be connected to them as they are usually used by attackers to install malware on the victim's computer. To enforce this, these devices should have pre-determined security controls that do not allow certain peripherals devices to be connected such as USB flash drives. If additional devices are needed such as a webcam, these should also be supplied by the school so that they can be whitelisted on the security controls or be whitelisted after approval if employee-owned. When performing work, employees must only store college data on the college-owned device, and must not perform any duties on a personally-owned device. Personally-owned devices are at a greater risk of intrusion and can cause great harm if sensitive data is stored on these devices or if connected to the college VPN. Finally, employees should treat their remote-work environment as if it were an on-site environment. To do so, employees should be wary of the same types of threats they might face on-site. Employees should always log off of their devices if not in use. Employees should never openly write down passwords, and be wary of shoulder-surfing if there are guests over the employee's home. These best practices can be further educated through a security awareness education and training program.

As much as employee workplace policies will enforce physical security, administrative controls are necessary as well. The laptops or computers supplied by the college should be the only devices that can connect to the school's VPN. This will ensure that any rogue device cannot connect to the VPN and potentially breach the entire school network through malware installed on the rogue device. To do this, the VPN should be configured with proper access control mechanisms in which only specific IP addresses or MAC addresses are allowed connection, followed by an implicit deny which will automatically deny any attempted connection to the

VPN if the IP address is not explicitly allowed. Also, management should actively run antivirus scans as a background process, regularly install important Operating systems and software updates in the background or when the device is not in use, and actively block malicious connections to websites.

One major issue that was analyzed within the realm of data was that there seemed to be a sense of too much availability to student application data within Slate. A new policy should be considered which requires Paige to manually audit the residual data within Slate and delete any data that is no longer needed or used. This audit should occur at least once a year, and this process would require the complete deletion of any student PII if that student no longer attends WPI or was never admitted. There should be no data within Slate on students that no longer have any affiliation with WPI.

These workplace policies and administrative controls will enforce stronger physical security in conjunction with a comprehensive security awareness program.

Network Security

The office has a VPN in place for the Work from the home policy during Covid. While this helps improve the network security there are still certain issues in the system. A single device being infected by someone who knows what to do can infect the entire server. This can be avoided by the office by taking simple steps. The steps needed to improve the network security should include making sure the VPN is enabled, backing up the data, having a firewall, and making sure the software is licensed and updated regularly with unused software being uninstalled.
The software on the company devices the employees have taken home should be limited to only ones necessary for their work and making sure their licenses and versions are updated regularly. The VPN should always be on whenever the devices are being used and that the data on the servers is backed up into an additional server that is disconnected from the network in case of attacks. There should be a network firewall in place to ensure security.

They should also have the necessary email and application restrictions in a place like following the DMARC protocol for opening emails and not opening emails not cleared by it. They should make use of a secure router and make sure the router does not work on parts like the WPA2 encryption which is relatively easier to bypass.

Operating System and Application Security

The office uses Slate to manage the application data and Acxiom to transfer the data over to Banner web using third-party encryption. The Student data on Slate is never cleared according to the office, which is an issue and the Slate privacy policy states the same. This means that if you even start an application but do not complete it, you might be vulnerable. This can be avoided by simply clearing the student application data every few years or after a designated period. The fact that Slate does not clear their cookies and cache make it even worse from the security point of view. The office should make it a point to regularly clean their application data and clear the cache and cookies as well. The devices that the employees use should all have a standard operating system with the necessary licenses and updates regularly implemented. The office should also make it a point to never declassify a student's data as private because that would enable Slate to use the data without incurring any legal issues.

Development Plans for a Comprehensive Security Awareness Program

User security awareness training and education are key to managing the new pandemic risks impacting the information security management process. Informed and educated users strengthen the overall security of an organization; while uneducated and disobedient users are a great risk. The Office of Graduate Admissions already lacks a strong security awareness and education program and the remote environment demands a comprehensive program to actively educate its employees on old and new threats.

Employees need to understand the security risks faced by their organization, indicators of these threats, and how to mitigate and report these threats as part of the program. They also need to understand the importance of security as a whole, and how their roles have a greater effect on the overall security posture of their department and the entire school. The Office of Graduate Admissions' attack surface is large and gives potential threat actors a variety of attack vectors mainly due to a lack of contingency plan, lack of department-wide accountability, and proven security concerns in their data management platform. Sufficient management-buy in will focus on these areas to build a proper security awareness program on top of regular training on current threats. To portray the security implications of these vulnerabilities to persuade buy-in, management must understand the risks of a potential security incident in each of these areas. A recent report from Ponemon Institute suggests that the average 10,000 employee company spends $3.7 million a year dealing with phishing attacks. Engaging in security awareness programs would typically improve employee security behaviors and can avoid such fines. The department of graduate admissions must analyze and make changes to security policies and procedures already in place. The policy should include firewall rules, system hardening standards, data retention policies, and password policies. The IT security department at WPI would oversee the campaign. They would effectively communicate the security policies and measures to employees by brief and informative videos, pamphlets, and an annual session where everyone gathers. The goal is to mitigate user risk, the program would help employees understand the role they play in helping to combat information security breaches.

A proper security awareness education and training program will focus on all of these points and more. Employees, however, need to receive training and education regularly. It is acceptable for employees to receive this training yearly, or once a year to keep updated on current threats and indicators of these threats. This timeline should not be neglected and should be enforced yearly, otherwise, employees will slowly become unaware of new threats and proper security best practices. These education programs should come in the form of modules in which they are delivered by video, and then further test the knowledge of employees by giving quizzes at the end of each module. Once completing all of the modules, employees will be given a certificate that will expire exactly one year after the date received to refresh their training and education. It is a continuous process to be accurately updated on new threats and techniques that arise each year.

As social engineering attacks become rampant, the office of graduate admissions needs to be security-aware. The department must be trained on spotting phishing emails, vishing, limit sharing of sensitive information about work on social media, and reduce the amount of information available to the public via their website. Providing staff members with regular training while raising awareness on security would minimize the risk of social engineering within the department.