MIS582 Team 1 Project
Rhode Island College Helpdesk
Final Recommendations

Team 1 Members:

Jonathan Duran
Justin Cabral
Humberto Martinez

Point of Contact:

Michael Caine: Technician Support Specialist I

April 22, 2022

Contents

Executive Summary

Based on our analysis of Rhode Island Colleges' helpdesk, we were able to identify numerous key areas inside the department that are doing an exceptional job at keeping their information security assets safe. There are great security protocols in place such as network segregation and segmentation that will not allow a bad attacker to gain access to the entire network if one computer were to be compromised. However, we found several areas that need to see significant improvement, or the department could find itself dealing with a major issue later down the line. One being the need to properly secure and dispose of hard drives that have critical personable identifiable information on them. Another being the need to upgrade the computers running Windows 7 inside the department to Windows 10 or newer. Under no circumstances should a department that is supporting other departments on a college campus be using an operating system that is no longer receiving security updates from its developer.

Our recommendations for each major part of the greater security infrastructure center around ensuring a comprehensive approach to security that relies on not just management taking responsibility, but students as well. Since student workers are relied upon heavily inside the Help Desk to provide support to faculty, staff, and other students at the college, we thought deeply about what measures should be put in place for them. Regarding some security recommendation implementations, they rely upon the Help Desk to make the case to the College Board to secure the proper funding inside the yearly budget. Since the Help Desk relies on a budget approved by the College Board, we recommended them to lay out a plan that correlates the cost of the security improvements, juxtaposed to the financial cost of a data breach. As we learned in this class, the cost of data breaches can far outweigh the cost of simple security upgrades. Our hope is that with the proper case made, they can secure the funding needed to ensure not only security inside their office, but on the greater campus.

The great news is that our point of contact, Michael Caine, is very willing and accepting of all outcomes that will come from this report. One of the most underrated aspects of addressing information security inside an organization is having those who lead it be willing, and active participants in maintaining its security. Michael played a key role in letting us meet with not only himself, but students to gather information on tasks that have changed since our previous employment there. We enjoyed our time working with him and hope to see the improvements made in the department in the future when we present to him these final security findings and recommendations.

Identification and authentication

The helpdesk uses a combination of magnetic key cards and a card access system as well as standard locks and keys to physically enter and open the office in the morning. The cards are used to lock the customer entrance at night and physical locks are used to secure the back door for the night.

Some vulnerabilities in these current systems include lost or stolen ID can be used to access the office, forged or stolen keys can be used to access backdoor and can be obtained from outside the office. Any employee that loses or misplaces their ID introduces a security risk to the assets contained in the office until they report their ID missing. While that keycard is unreported, it may be used to enter the building and the office. Secondly, the physical keys used to unlock the back doors to the office are standard mechanically cut keys. Any individual that has access to the key unsupervised may take a photo of the key and make an unauthorized copy of the key. The lock of the door may be compromised using traditional lockpicking techniques. Lastly, any lost or misplaced keys may be picked up by any individual and used without any record or log of the key being used. Any holders of the key, which include office full-time staff and campus security personnel may introduce a vulnerability anytime that key leaves their person or leave them unattended.

Some unusual information security threats in this area include keycard access not granted at the discretion of the helpdesk staff, and keycards are occasionally shared or borrowed between full-time and student technicians. The first threat involves the information security team at Rhode Island College being responsible for key card access being applied to employee IDs across the campus. If any security breach occurs regarding keycard access in their department, it is out of the control of the helpdesk staff. Finally, occasionally, full-timers may lend some student technicians their keycard if a situation presents itself. In the rare event this happens, if a student technician decides to act maliciously with the keycard, there is nothing in place to prevent the student's activity.

Recommendations: The helpdesk can remove the risk of someone making a duplicate key and entering the office by installing a key card access system lock on the back door, retiring the standard mechanical lock in place now. This will ensure that the only people that can lock and unlock the doors to the offices are helpdesk technicians, and any campus security officers. Since there will be no physical keyhole, any person looking to manually penetrate the lock housing will have to carry more obvious equipment, creating a passive deterrence for malicious actors, as they risk being identified if they try to break open the lock. If a card is lost or stolen, communication should be established with the Information Security team to disable the card’s access privileges in a timely manner.

To address any keycard access concerns, better communication should be established between the IS team and the helpdesk. The helpdesk should investigate making keycard access be a part of the new hire onboarding process. In addition, student technicians should be given keycard access to prevent card sharing between full-time staff and students. The helpdesk should coordinate with the IS team to receive a copy of any audit logs available from the keycard access system. This can be used to deter theft and be used in investigations. If any equipment leaves or goes missing, the logs can be used to determine who last unlocked the office and at what time. This would help create a trail for employees or other investigators to follow, if there were incidents where an employee’s keycard was used and either the employee was not physically there, or they reported it missing and someone else had used it.

Authorization and access control

The helpdesk employees each have distinct roles and levels of access and abilities. Depending on their roles they may have access to different programs and tools such as active directory, Microsoft System Center Configuration Manager (SCCM), JAMF, and the ability to remote into computers and assist users. Access to some of these tools is implemented using an access control list where an individual's network account is given access to use these tools.

A vulnerability in this type of control method includes compromised accounts that can be used to maliciously take advantage of their access to these certain tools, also there is no type of physical access control in place that prevents anyone from walking into the helpdesk office and using one of the logged in workstations within the help desk. This means anyone could walk in and if one of the workers has left their computer unlocked or if the intruder accesses one of the office's general workstations that is usually logged into for typical use by any of the employees, they can remote into any of the colleges computers and manipulate, steal, or delete whatever files they can get their hands on.

One of the unusual information security threats faced by the organization is student workers all log into the front desk workstations using the same username and password and usually do not log out between shift changes, these include the stations specifically used for remote access into windows PCs and Apple computers. Another of these unusual information security threats is the lack of physical access control that exists for individuals entering and leaving the helpdesk office. The door to enter the help desk is usually left open for the public to enter, this leads individuals to the front of the office where the student workers' area is located. There is no physical access control between the front area and the student workers' area, just a small 3ft wall that has an open side entrance. If anyone who walked in during a time where either there were no student workers present or simply walked past an unsuspecting student worker and gained access to any of the unsecured workstations, they could conduct various forms of malicious activity.

Recommendations: To prevent someone from using a logged-in workstation, the helpdesk should take advantage of the standard issue keyboard's function keys. The Dell KB216 has a function shortcut to lock the computer it is connected to with two button presses. Technicians should be taught to immediately lock their computer anytime they must leave or get up from their workstation. Student technicians should be moved away from one standard shared account and use their personal unique domain accounts. This will also create an auditable trail of who is using what computer during shifts. This would also help in managing and controlling access for individuals who leave or are no longer with the organization, since with the current structure anyone who leaves or quits will still know the credentials used to log onto these computers, which they can then use if they every sneak back or steal one of these stations. In moving away from a shared account to unique domain accounts, this would allow the ability to add and remove access from student workers once they leave or quit. They could be added to an access control list while working then removed once they graduate and leave the helpdesk or quit. This would mitigate against potential incidents where a malicious student worker who was fired or quit could still have access to these stations, or in a scenario where the username and password for this shared account was leaked and compromised.

To provide more physical access control and prevent the possibility of someone walking into the student worker area unauthorized, the helpdesk should place a more significant barrier that limits access from the front of the office into the rest of the office. Currently the 3ft wall that only

partially covers the front of the office leaves a big open space for anyone to roam past the front and into the student worker area, the full-time employee's area, and even the back office where most of the equipment and computers are stored. This type of physical access control could be implemented by adding an extension to the current 3ft wall they have that would include a gate that can be locked from the office side of the wall. This would prevent and deter people from trying to cross or enter the rest of the office. On this gate the helpdesk could also install a sensor or bell that emits a sound every time the gate is opened; this would alert the staff to anyone who is entering from the front of the office and would prevent someone from trying to stealthily enter the office and steal or do nefarious activities.

Auditing and accountability

The helpdesk uses tools for remote computer problem assistance. These tools include Microsoft System Center Configuration Manager (SCCM), JAMF Remote Desktop, and Extron Global Viewer. To use these tools, a technician must use specific user credentials depending on the tool. The helpdesk is also responsible for servicing and rolling out new computers for users on campus and retiring old machines with their hard drives. The drives are kept in the office and the technician responsible for moving the drive must sign their name on the drive and the date it was retired, where it is kept until its destruction 6 months later. The office also uses Team Dynamix for support ticketing. Every technician should have an account to create and modify tickets.

Currently, the office does not use the logging features present in any tools for remote assistance. The process for logging in does not require any multi-factor authentication, meaning if someone’s log in credentials is compromised there is nothing stopping a bad actor from using their credentials. JAMF Remote Desktop and Global Viewer do not notify the user if a technician has remoted into their equipment, allowing anyone with log in credentials to potentially spy on a user’s activity or disrupt their workflow with remote commands. Additionally, the office does not always lock the cabinet with retired hard drives in the office. The drives are not encrypted, and their contents can be accessed with a simple SATA drive reader in the office. Any student worker or bad actor who could enter the office could view or steal confidential information of users on the drives. It is also common for some technicians to log retired drives on behalf of other technicians if they are busy with other tasks. This means a technician could retire equipment and log their work like someone else, resulting in another technician being blamed for the work of another's if their work was done incompetently or maliciously.

The tools used by the office are not in complete control by the help desk staff. In the case of JAMF and SCCM, only the Information Security team can make changes to the helpdesk technician's permissions, including viewing and enabling logs of user’s activities within the two tools. Global Viewer is an AV equipment remote tool and the capabilities for enabling security logging and multi-factor authentication have not been enabled yet by the company responsible for developing the tool.

Recommendations: Addressing these issues will require assistance and collaboration with the Information Security team. Multi-Factor Authentication is supported by JAMF so the helpdesk should work with the IS team to require it when a technician needs to remote into a user’s computer. In addition, the Helpdesk should request that remote connection prompts be enabled in JAMF to notify users when a technician is attempting to remote into their computer. This will address any concerns with a technician performing malicious actions with their JAMF

capabilities. If a technician knows that a prompt will appear anytime they attempt to remote into a computer, they will not attempt to use the functionality to steal or spy on a user.

To address issues with retired hard drives, the helpdesk should begin locking the cabinet they are stored in and making one technician responsible for locking and unlocking the cabinet. The helpdesk should also adopt a new process for retiring hard drives to create more accountability and prevent data theft. The reformed process should potentially involve attaching the work order ticket to the hard drive when it is retired, so there can be an online, verifiable copy of which technician completed the workstation retirement. Since the office only completes around one to five retirements a day, requesting the cabinet be unlocked after they have completed their task should be a simple change that is easy to implement. This change will also deter any technicians from stealing hard drive data after it has been placed in the cabinet. Lastly, the help desk should encrypt the drives following their retirement to provide an extra layer of security in case the cabinet is compromised.

Cryptography

The help desk utilizes remote desktop (RDP) and Apple remote desktop to assist users remotely and help with client issues from connecting printers, mapping network locations, and other tasks that can be done from the help desk office. These two software tools both employ the concept of protecting data in motion. During the connection data being transmitted over the network is encrypted and kept secure from any eavesdropper who might be scanning the Rhode Island College network. Both tools employ different encryption schemes such as AES and SSL/TLS for the data being transmitted during the remote connection.

Some of the vulnerabilities that might be present with these tools might be the lack of security configuration and updating the settings of this tool to keep up with new and evolving threats and vulnerabilities. Currently there is no designated process to update the security behind the application to make sure the encryption settings are up to date, also the specific use of SSL/TSL is usually set to an outdated version, which may be vulnerable to attacks. Since most of the student workers have limited knowledge of the cryptographic setting and vulnerabilities associated with the different options of this tool, they do not configure the application prior to utilizing the RDP application.

An unusual information security threat faced by the organization relating to cryptography includes students emailing their sensitive information, such as social security numbers, addresses, and state and federal ID card information over unencrypted email. This usually occurs when a student is an incoming student and is trying to create their Rhode Island College student account. They usually misinterpret the automated emails sent when they are accepted into the college and begin sending this type of information to the Rhode Island College help desk email in hopes of expediting their account creation process. This results in the help desk employees calling or replying to the students that they should not be sending this type of PII over an unencrypted email communication. The employees do not have specific instructions to delete or quarantine incoming emails that contain this information and usually just let it sit in the helpdesk email inbox. This presents the issue of data security, specifically for data at rest. While these emails sit for an unknown amount of time on the college's email server, an attacker who manages to breach or compromise this account can then begin extracting all the unencrypted PII.

Recommendations: Regarding the different remote assistance applications, there should be a script that automatically looks for updates to the application every so often, once a week. This script could run at a designated time, such as off-hours, so that any updates would not interfere with productivity for the employees during their work hours and prevent them from assisting users. This recommended action would help ensure that the necessary encryption settings would be up to date and any vulnerabilities from older versions, that may allow for the encryption or communication during remote sessions to be compromised, would be patched and fixed. The helpdesk currently has a full-time employee who writes scripts for various other applications and thus creating one for this case would not be something that would be extremely hard to implement. Regarding student workers not having the knowledge to configure these applications prior to using them, there should be a set of physical instructions that a student worker could access and use to configure the applications prior to remoting into a user's computer. This could be placed in an easily visible bin or next to the primary station that is used for remoting desktop assistance.

The recommendations for the helpdesk also include working with the admissions department to inform students who have been accepted into the college not to send any type of PII information over unencrypted email. This would help reduce incidents where unencrypted PII data can be stolen during these unencrypted communications channels. Currently, the admissions email that is sent out does not notify students to not send PII data to the helpdesk for their account creation process. This collaboration would help reduce the number of new students who send this information without knowing the potential consequences this might have. To protect the current data at rest, the helpdesk would need to work with the networking department to ensure that any emails that may contain PII and are stored on the email servers would be encrypted for a limited period and then deleted once they are no longer relevant or necessary. This would prevent or mitigate against an attacker from gaining access to these email servers and stealing unencrypted PII data.

Operations security

The helpdesk is responsible for retiring and replacing workstations of employees on campus. The helpdesk identifies the need to protect the confidential data of employees left behind on retired computers. The old hard drives are in a lockable drawer in the office and are kept for at least 6 months, and then are destroyed to ensure no malicious actor may find them in a landfill or trash receptacle. The office is also responsible for preparing all computers on campus, including lab computers with expensive software for educational use. The office identifies the need to ensure no software license or computer can be stolen or used outside the campus. The helpdesk has all software on campus paid and authenticated through a network license that requires a connection to the on-campus network every 6 months for the software to remain functional. Lastly, the office consistently receives phone calls for assistance in setting up student and faculty accounts, like first time password setting and MFA onboarding. The office identifies the need to assist students and faculty with their issues, or else risk a large population of the college's data and PII. The helpdesk technicians always assist students and faculty with issues and provide guidance and tips to ensure their accounts are secure. Additionally, all technicians are required to make it clear during any communication that there are no social security numbers. passwords, or any PII should be given to any technician at any step of their assistance.

As mentioned previously, various vulnerabilities exist within their system for addressing their retired data. The drawer where the hard drives are kept is not always locked, allowing any student technician or malicious actor to grab one when a technician is not paying attention. The drives are not encrypted while they await destruction, meaning any person with access to the drive may view its contents. For their process of securing software and hardware, any malicious actor that may steal a computer or somehow install software using the network license may work around the network requirement by occasionally visiting the campus and plugging in the stolen hardware in question using any spare ethernet port on the campus. During regular business hours of the campus, various classrooms are left unattended with spare ethernet ports with network access available. Lastly, no technician on a phone call or working with a student or faculty member is not monitored during their conversations when assisting with account issues. If any technician receives or views any PII of a user, unless they report their actions themselves, there is no process in place to deter technicians stealing/harvesting PII of the users they assist.

Faculty and staff of the college consistently use the backdoor entrance of the office as an entrance to the building the office resides in when the front door is not open, or out of convenience. The technicians attempt to notify the faculty and staff that the office is not meant to be used as an entrance to the building, but do not have the authority to remove any person or penalize any person for refusing to use a different entrance. Any person could walk into the office during business hours and pose as a faculty or staff member to view the process or PII of a user. The malicious actor could also place a bug or other listening device to overhear any plans to change the operational security processes.

Recommendations: Locking the drive cabinet and encrypting drives after they have been retired should prevent any theft of data from a technician or any person attempting to read the drive from the cabinet. This operational security measure would help to mitigate the current vulnerability that leaves this sensitive data open for anyone to handle. The helpdesk should investigate if the network license authentication window can be shortened to once every month or a similar time frame. This will prevent license theft. The helpdesk could also investigate the costs for maintaining recordings of all phone calls made to the helpdesk. This will create an auditable database for every technician and will deter any technicians from stealing or harvesting data of users through the phone. If any situations arise with hostile language being used over a phone call, or disputes with someone's behavior, the phone recordings will provide an effortless way to discover who is at fault in a situation as well.

With respect to the unattended ethernet ports in the various classrooms and budlings on the college campus, this potential vulnerability against critical network information should be mitigated by working with campus security and the different departments to instruct professors to close and lock these rooms once they finish their classes. Since most of these classrooms are now keycard access enabled, there should be a way to implement and enforce the ability to automatically lock these rooms after a class is over. This would help ensure that countermeasures are in place to prevent anyone from accessing these rooms and accessing the ethernet ports within them. In addition to the physical countermeasures the helpdesk should implement port security on ports that have permanent computers or devices, such as printers or other network devices that are in public locations. This would prevent someone from unplugging the device connected and utilizing the port to gain access to other critical information. With port security the ethernet ports are configured to only allow specific MAC addresses that are designated to be plugged into these ports to access the internal campus network, all others will be blocked.

Physical security

The Rhode Island College helpdesk does employ all three forms of physical security controls which are deterrent, detective, and preventive measures. For deterrents, the helpdesk has signs posted on both the back employee entrance and the front public entrance. The sign in the rear entrance that is strictly used by employees has multiple signs that indicate the entrance is for employees only and not for the public to use, it also displays alarm company logos which alert individuals that the entrance is protected by an alarm system. One of the major detective controls that this organization relies on is their physical intrusion detection system, this is set to be activated during off-hours once the helpdesk closes. The system is activated once all the entrance and exit doors in the office have been locked and secured. This system monitors unauthorized activity once activated such as doors opening and windows being damaged or other unusual activity and reports this to the campus police who can then come and investigate any potential physical security concerns. Lastly, the preventative control used by the helpdesk to prevent unauthorized individuals from entering either through the employee entrance or during non-business hours are the mechanical locks on the physical doors. These locks can be either locked from the inside or from the outside with one of the physical keys.

Within these processes for physical security there exist vulnerabilities that may potentially impact the information security of the helpdesk. For example, the alarm system, which is the detective control, will only be activated if all the doors of the office are closed and locked correctly. This system relies on the last employee who is leaving the helpdesk at the end of the day to verify and manually close and secure every entrance and exit in the office. This leaves room for error and the possibility that an employee who is in a rush to leave may not physically check and lock all the exit and entrance doors and thus the alarm system will not be activated, allowing unauthorized individuals to enter the office during non-business hours and when the helpdesk is empty. The second vulnerability is the mechanical locks for the entrance and exit doors. The way these doors lock is by one of the employees manually using the keys for the doors and locking them. There is a vast amount of room for error in this process such as one of the employees, who has a copy of this key, losing the key and falling into malicious hands.

One of the unusual information security threats faced by the helpdesk is that some of the back entrance doors are infrequently kept open during days when individuals must transport equipment during the monthly electric waste disposal or to transfer it to other locations. This leaves the opportunity for an unauthorized individual to use these doors to walk in unsuspectingly and either steal or tamper with equipment that is left unattended. Also, this leads to the area in which Rhode Island College employee machines are being troubleshot for issues, thus any unauthorized individual who uses this opportunity to enter can get access to these computers.

Recommendations: If the helpdesk can arrange for the keycard access system locks to be installed on the back doors, this should make locking the doors at closing time easier for all technicians responsible for closing the helpdesk. The helpdesk should investigate its options for also leaving the back door always locked to prevent any outside individuals from walking in the office or using it as a back entrance. If all technicians always have their keycards on them, leaving the backdoor locked should not prevent any technician from entering while also preventing malicious actors from slipping in when attention is elsewhere. This can also ensure the back door is locked at closing time, as no technician will need to remember to lock it. If locking the door is not an option, the help desk should coordinate with campus security and the Information Security team to investigate if automatically locking the door after a certain period is

an option. If the door can automatically lock itself five minutes after closing time, the risk of a technician forgetting to lock the door at closing time is significantly mitigated. Any malicious actor looking to enter the office will need to be at the office within five minutes of closing time.

Regarding the back entrance doors leading into the storage area being kept open during the monthly electric waste disposal, there should be a policy in place that would require at least two individuals to work together during this required monthly task. In this situation one person would transport the equipment, while the other would stay and organize the next batch of equipment to be transported, while also maintaining a presence at the back entrance to deter someone from entering while the doors are kept open. Alternatively, the policy could state that if only one person is available for this task, that the person must close the doors during each trip to prevent any unauthorized entry into the bay area of the helpdesk.

Network security

The network security processes in relation to information security inside the help desk start with using static subnets to segment the network to mitigate risk. The helpdesk computers are hosted on the ric.edu subnet which lets them support most of the college campus, but there remain some legacy systems that are mapped to an older ricol.edu subnet. Printers that are used inside the office are on their own subnet as well, along with Dynamo label printers, and fax machines. These subnets are protected by firewalls to segregate the covered devices from the public Wi-Fi on the college campus. The subnets also allow for easier analysis of inbound/outbound traffic when searching for rouge or malicious actors.

Inside the network security processes used by the help desk, there remain possibilities of vulnerability exploitation due to some reliance on legacy systems. For example, the ricol.edu subnet which the helpdesk uses to support the more administrative processes at the college does not use the same server-side role-based permissions system as the newer ric.edu domain. This leaves the door open for rouge actors who know local administrator passwords to modify vital systems on the network without raising flags. If attackers were to use this to gain access to the helpdesk computers through the ricol.edu subnet, they could assert control of a vital piece of I.T. infrastructure or lay dormant to find bigger targets inside the network that the college depends on heavily.

An unusual information security threat regarding network security that is found at the helpdesk is the possibility for someone to access computers remotely without handshake verification. This remains because some machines still support the ricol.edu subnet, and all it would take is for someone to know the name of a Windows PC inside the help desk. Any user on ricol.edu can use $(PC Name) in the run application on Windows to silently remote into the given computer. This poses all sorts of risks to personable identifiable information found on help desk computers. An attacker could install malware to lay dormant, and since help desk computers are the ones who normally remote into other computers on campus, they could scrape keystrokes, email addresses, and other critical information.

Recommendations: The helpdesk should coordinate with departments on campus to speed up retiring the old ricol.edu subnet and migrating them to the new ric.edu subnet. The helpdesk should help discover what these departments need to expedite the process and assist in any way they can to prevent any vulnerabilities in the old subnet from being exploited. Once on the new subnet, its role-based permission capabilities should prevent any risk of local passwords being

used to modify vital files or systems on the network. This will also prevent any unauthorized remote access attacks.

Along with better coordination among departments on older subnets, the Help Desk should install software that logs anyone who attempts to use the $(PC Name) to silently remote into computers without the proper handshake. Depending on how long it may take to update all machines to Windows 11, this is a key addition that's needed. This feature would help increase network security and keep a list of everyone who attempted to use it for malicious purposes. Once the ricol.edu subnet has been deprecated, there will no longer be a need for the logging software.

Operating system security

At the Rhode Island College Help Desk, most computers are managed through SCCM, which installs Windows and deploys it. The advantage of using SCCM is that it allows the SCCM lead at the help desk to push emergency patch updates to Windows across the campus if a serious enough vulnerability is discovered, such as the printer spool bug that plagued Windows machines in 2021. However, not all machines use Windows 10. There remains one computer that uses Windows 7 because it is the designated one which is used to remote into the payroll office when support is needed. Some computers at the helpdesk also run macOS, with the operating system and updates being deployed using JAMF. The computers at the help desk and on college campus running macOS only get updated the following year of a major release version.

When it comes to the operating system security at the help desk, there are some vulnerabilities that remain in-house due to the stagnation of release updates caused by older machines. While the SCCM manager can push out emergency patches to the Windows 10 computers in the office, they cannot upgrade directly to Windows 11 because most of the machines in the helpdesk are not new enough to support Windows 11's TPM 2.0 requirements. This leaves the door open for potential attackers to use a Windows 10 zero-day exploit to cause harm to systems and extract vital personal identifiable information. The same can be said on the macOS side, however, most of the Mac computers on campus are routinely upgraded through special grants. Whereas the windows machine updates are more closely tied to the college's budget, which makes planning for bigger upgrades a challenging process.

Unusual informational security threats relating to the help desk include the prolonged use of Windows 7, long after it has been dropped from security updates by Microsoft. In just the past 6 months, over 50 more vulnerabilities have been found inside Windows 7; everything from the printer spooler elevation of privilege vulnerabilities to the exFat Filesystem disclosure vulnerabilities. Using an operating system that has been deemed "unsupported" by Microsoft since 2020 is just asking for trouble. Especially when you consider that the payroll office is the main one connecting to the machine inside the helpdesk office. The value of the critical information in that office is something an attacker would absolutely target, and it is a place of contention inside the helpdesk as to how they need to communicate this with higher ups to resolve this at a budget level.

Recommendations: The most important recommendation that we can make for operation system security is for the Help Desk to upgrade all machines that are not capable of running Windows 11 due to the TPM 2.0 requirements. Although the machine updates are tied to the college budget, we believe if a proper case is laid out that puts in perspective the overall financial

and reparatory risk, then money could be allocated for an internal department upgrade as well as campus wide. Any monetary cost up front to upgrade machines dwarfs in comparison to the financial damages, as well as reparatory damage the college could face if a data breach happened due to outdated operating systems.

Another recommendation is to work with the payroll office to phase out their computers that run Windows 7 and get the proper software that is compatible with a newer version of Windows. The sole computer at the Help Desk running windows 7 is a ticking time bomb and should be addressed as soon as possible. We recommend that the Help Desk lay out a financial plan for how much it would cost to upgrade the Help Desk and campus to newer machines, and how much it would cost the college if a data breach occurred. By putting those two juxtaposed to each other, we believe it will help them secure the proper funding inside the budget to make the changes needed to increase the overall operating system security inside the help desk.

Application security

The Rhode Island College help desk installs all applications on Windows 10 using SCCM. This not only keeps all applications up to date, but it disallows any full-time staff, or student workers to install software downloaded from the internet without the proper permissions. Similarly, the computers at the help desk running macOS all have applications installed using the JAMF manager. This too shuts down the possibility of rouge applications being installed on the computers. There are exceptions, such as Extron Global Viewer, which uses a web browser to interface with the web application to manage all the projectors and I.T. racks inside classrooms on campus remotely. Another exception is that those machines running on the ricol.edu subnet can use local admin passwords to install rouge applications because there are no network permissions associated with that domain to restrict that behavior.

The vulnerabilities that exist inside their application security process mostly involve the use of the older machines which do not have safeguards against installing applications if the local admin password is known. Since all student workers know the local admin password for these machines, it raises a risk that students could inadvertently install malware which could disrupt one of the critical systems at the helpdesk, which is supporting the payroll office. Allowing anyone with knowledge of an admin password to install any software they want is leaving the door open for bad actors. Though the college networks are segmented, malware could lay dormant for weeks, months or years updating itself until the time is right to extract information.

Since Global Extron Viewer is a self-hosted web application inside the helpdesk on a server in the back room, there are unusual information security threats regarding accessing the website. Since the website is older, it does not have the correct CSP (Content Security Policies) or CORS (Cross-Origin Resource Sharing) to prevent cross-site scripting attacks or cross site request forgery. This provides attackers with an avenue to attempt to gain access to the server, and eventually to all those who connect to it. Since student workers are routinely connected to monitor classrooms, this oversight is one that must be fixed to avoid a potential disaster.

Recommendations: To ensure greater application security, we recommend that the Help Desk remove all local admin passwords from older machines that are not part of the ric.edu subnet. Local admin passwords pose a significant risk due to the ability for a Help Desk student worker to install any applications from the internet. Although older machines on the ricol.edu subnet are not part of SCCM (System Center Configuration Manager), it is still possible to remove local

admin accounts and create a server role for only authorized full-time workers to manage these machines. Not doing this leaves the Help Desk vulnerable to potential malware installations by student workers that could disrupt service not only at their office, but the college campus at large.

Another recommendation we have is for the self-hosted Global Extron Viewer server and website to adopt the proper Content Security Policies and Cross-Origin Resource Sharing policies. With the proper CSP and CORS in place, the Help Desk will mitigate the risk of any cross-site scripting attacks or cross site request forgery. Since the Global Extron Viewer manages all the projects and I.T. racks inside classrooms, this is an important vulnerability to close because if exploited attackers could cause classes to be severely hampered due to their reliance on projectors and computers.

Development plans for a comprehensive security awareness program

With the Rhode Island College Helpdesk development of a comprehensive security awareness program, this would help mitigate potential risks that might impact on the information security management processes that the helpdesk currently employs. For an organization that deals with helping users with their hardware and account issues, a stronger security awareness program must be established to ensure that the PII and sensitive information of their customers are not compromised or used for malicious purposes by technicians within the office or outside malicious actors exploiting flaws in their current processes. The reformation of their processes when retiring equipment and the addition of a few additional security measures, like expanded key card access, are simple on paper, but can go a long way in securing the information the office is responsible for.

Technicians must acknowledge the responsibility their job requires and adapt their workflow to accommodate more security checks. They must recognize the risk they potentially pose to the helpdesk customers and how to mitigate and report any activity that may jeopardize the security of the helpdesk and their customers. All helpdesk technicians must be ready to accept more responsibilities to ensure the safety of the equipment and operation of the helpdesk, like one technician being responsible for locking and unlocking the drive cabinet, or all technicians accepting their phone calls being recorded, and the potential for more effort in closing doors when not in use or while unattended and reopening them when they return or have someone who can attend to the entrance. In addition to accepting more responsibilities, all technicians should be prepared to communicate more often with outside departments of Rhode Island College to facilitate better security practices that could benefit the helpdesk, like the campus police. Information security, or network and telecommunications team.

A stronger security awareness program should address the current vulnerabilities within the core areas and be able to adapt to future ones. Technicians should receive training and adapt their current processes to deal with users and their issues and address current vulnerabilities within their methods of communication and dealing with accidental PII being disclosed and implementing monitoring to their lines of communication with customers, like the phone call recordings or email communication. Technicians should also address physical concerns like locking cabinets or entrances and exits more frequently to ensure workplace safety as well as physical safety of data and information. Stronger relationships with outside departments like the campus security and information security teams should be maintained after being established to

enable more oversight to tools used by the technicians if necessary and better physical protection of the office space.

Description of how you conducted the analysis and recommendation processes

All team members felt comfortable partnering with the Rhode Island College helpdesk, as all were student technicians at one point. We all spent some time in person speaking with the current employees and asking them various questions about their information systems, networks, and the processes the helpdesk employed that we thought might be essential in understanding the information security practices that could help us during this project.

For our analysis during this phase, we used recent knowledge of the tasks and practices we did while we worked there and saw how some of those have changed and stayed the same. We shadowed some of the student workers to see how they spent their shifts and how similar or different the student work schedule and practices were. We spent time seeing how they went about dealing with user requests, issues, and what tools they used to troubleshoot or solve the problem the users needed help with. We also spent time seeing the tasks and practices of the full-time employees, we saw how they handled the more complex tasks of creating work orders, managing accounts, and other full-time processes.

For our recommendations, we brought together all the material and knowledge we collected from observing the helpdesk and our prior knowledge working there. We combined this with the knowledge we gained from our graduate experience taking this information security and other security classes, to identify and point out parts of the help desk processes that might need to be changed or updated to reduce some of the information security vulnerabilities. We evaluated all the current vulnerabilities and met as a team to collaborate on what ideas and topics from the material we learned in this course could be used to help the Rhode Island College help desk reduce the number of vulnerabilities they have and provide better information security in their workplace and for their employees. We consulted with our contact at Rhode Island College to help assess what were the most significant vulnerabilities and establish reasonable recommendations for them.

Acknowledgement of supervisory responsibility for each component

Jonathan Duran

- Cover Page
- Authorization and Access Control
    - Recommendations
- Cryptography
    - Recommendations
- Physical Security
    - Recommendations
- Description of how you conducted the analysis and recommendation processes.

Justin Cabral

- Network Security

    - Recommendations
- Operating System Security
    - Recommendations
- Application Security
    - Recommendations
- Executive Summary

Humberto Martinez

- Identification and Authorization
    - Recommendations
- Auditing and Accountability
    - Recommendations
- Operations Security
    - Recommendations
- Development Plans for a comprehensive security program
- RIC Helpdesk communications liaison
- Table of Contents