The Information Assurance Perspective of the IT Department of a High School

Rafael Marques Braga
School of Electrical and Computer Engineering
University of Miami
Miami, FL
rxm403@miami.edu

***Abstract*— In this paper, an overview of the information assurance of a high school was studied, mainly focusing on its network and technological side. When looking at every asset a high school has on its technology sector, different vulnerabilities and threats are studied. To ensure these vulnerabilities are dealt with, some controls and recommendations are then presented along with the costs to put such recommendations in place.**

Keywords—Information Assurance, integrity, confidentiality, availability, threats and vulnerabilities, controls

I. Introduction

Every business and corporation today have to hold massive amounts of private data. Users expect this data to always be private, accurate, and available to them at any time. This is why the three main security requirements for any type of information are: 1) secrecy and confidentiality, 2) accuracy, and 3) integrity and availability.

These 3 pillars of information assurance are essential to be considered when looking at possible vulnerabilities, threats, and the countermeasures that are taken when considering the purchase or use of any asset in a company.

In this paper, the security concerns will be examined when assessing the information assurance side of a theoretical semi-private high school – The Infinity High School.

This high school is a school with around 300-400 students, as well as teachers, staff, management, and an IT department. Parents' information is also examined and assessed in this paper, as the school holds additional critical information from them.

II. Stakeholders

For this specific report, it will be looked at in the point of view of the IT (Information Technology) department in the high school. The IT department is extremely important when talking about the information assurance. Even though this is not the department that is collecting the data (such as bank accounts, employee's information, papers, and grades, etc.), this is the department which has to manage all of this data. The IT department has to keep all data secured and always available to either the students or management office. This same department also has to always make sure the data is secured and as accurate as possible.

Almost every single organization today has to have an IT department since this specific part of the company holds and manages essential assets for the proper functioning of the school. This department is extremely important in this day and age since most of the data held by a high school is digital. This includes all of the employees' information they hold, the students' work, information from the marketing and admissions department of the school, emails, and the information from the high school's website. All of the assets needed to keep this information safe and properly organized needs to be maintained and kept up to date. This is all part of the responsibility of the IT department.

III. Current Environment

For the purpose of this paper, an initial environment is set up so the state of the high school is known. This includes the infrastructure that is already set up for the high school, what it has, and what it does not have. This is noted down, so it can then be studied and analyzed. Then, all the assets, threats, vulnerabilities, and counter measures are examined in order to keep the high school functioning as well as possible.

For the Infinity High School, it should be noted that the school has a computer lab with desktop computers (connected through a wired connection to the network), a printer, and an external internet connection. It is also assumed that the school has a website for its visitors as well as an internal page containing school related events and information.

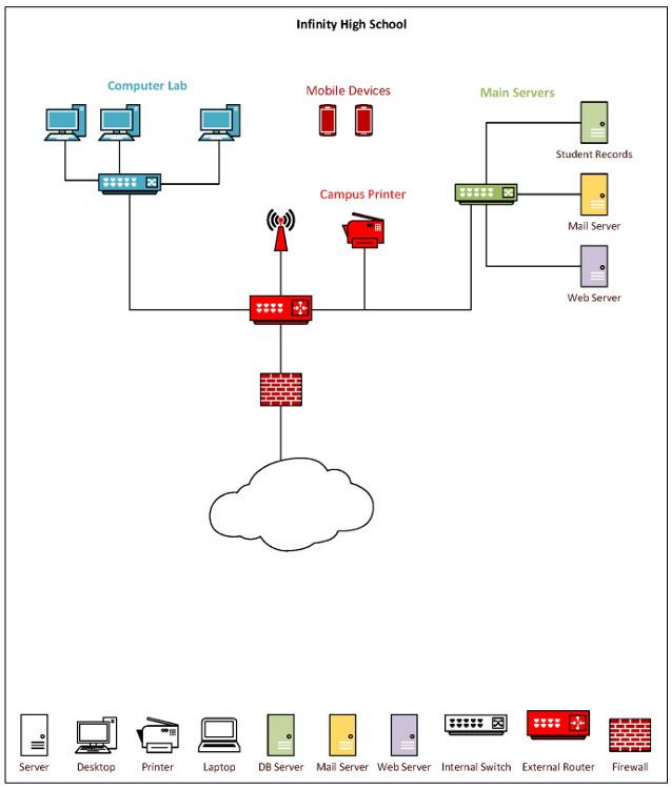
For the student and employees' digital records, such as demographics and grades, the school holds a special database so the data can be securely stored. To have access to this information, students and parents were provided with a username and password. Faculty and staff were also issued usernames and passwords to allow them to access appropriate records. However, faculty and staff are able to update/read/write all the records in the database, while students and parents are

only able to read their appropriate records. Faculty and staff are also provided with school email addresses in order to communicate with the rest of faculty, students, and parents.

Lastly, for the school network, the campus is set up with a wireless mesh network to allow everyone to access the local school network. This is an open unsecured Wi-Fi. This is so the students can start to bring their own devices to campus, including phones, computers, and tablets.

An external firewall is also added to the network with some simple rules to allow outgoing traffic with NAT and incoming traffic to the website and email but blocking all other incoming traffic. Image 1 shows a brief summary of the network organization of Infinity High School.

IMAGE 1 – INFINITY HIGH SCHOOL NETWORK



IV. ASSETS

In terms of assets, the IT department holds a variety of equipment, assets related to the infrastructure, and digital assets for connectivity and personal use. For this, the assets are divided into 3 categories: Physical, Personnel, and Informational assets. These will be listed below and classified by of how their level of importance. Assets can be classified into critical, intermediate, or informational.

Critical assets are the assets which are important for the operations of the high school; namely, operations cannot continue without them. Intermediate assets are those which are important to operations, however, are not as critical. Even though operations from the high school can continue without them, operations will be a lot slower. Informational assets are the assets which are important, but infrequently used or not essential for operations. Therefore, operations can continue without them in case something happens.

A. Physical Assests

1) Infrastructure: These are all assets related to the hardware and systems for the high school. These include the infrastructure hardware such as computers, routers, switches, cables and firewall equipment. These are all critical assets to the school, as the network is what holds all the school together. If the infrastructure to the school is down, it means students are without internet, teachers cannot acccess their teaching material, staff cannot access their data, and parents cannot access the portal for the school.

2) Internet Connectivity: The internet connectivity is considered to be the IT department's asset since the IT department is the one responsible for its management and availability. It is another critical asset for the school since today most of students and management are dependent on the internet. If it goes offline, most operations for the school are completely halted and teachers need to teach their material in the old school manner without the assistance from softwares like Zoom or the aid of educational videos from the internet.

3) Facilities: Facilities such as the computer lab, server room, and firewall rooms are part of the IT's assets. Even though these assets are critical for the operations of the school, they always need to be in a stable and protected environment. In case of a fire or hurricane, these rooms should not be easily burned or flooded, as these rooms hold all the network hardware, infrastructure and internet connectivity going.

4) Software Licenses: These are a subset of the infrastructural assets; however, these are mostly considered to be of intermediate importance. Many softwares for a school from the Microsoft Suite or mangement software, for example, are extremelly important for the school. However, if software licenses for programs that are only used by one department (e.g. MatLab), this would not stop all school operations and therefore are not rated as highly in importance.

B. Personnel

1) IT personnel: The IT personnel is an important asset to keep all the instruments online. Even though the team as a whole is considered to be a critical asset, each individual person is only considered to be an intermediate asset since the team should still be able to function without a sick employee or without a employee who is changing jobs.

C. Information

1) Data: All the data that the school holds is considered to be a critical asset as well. These data servers contain all the emails, student grades, payroll statuses, employees' demographic information, and teachers' class material. However, if individually classified, assets such as demographic data can be classified as infomational, since if this information is lost, it can be easily acquired again by sending an email requesting this information to the employees and not much impact is done to the day-to-day operations. However, some of

the data is considered to be critical (e.g. bank accounts and payroll information). If such data is stolen without any encryption, employees can easily lose money at the school's cost. Emails and their back ups are considered to be an intermediate asset since, if lost, it can affect some operations in the long term, but it will not do anything to stop all operations in the school.

2) Online Portal: The online portal is also a critical asset for the school since this is the interface between students and teachers. This is how professors assign their homework to the students and how the students submit their assignments. Without the online portal, students are not able to see their grades, submit their assignments, or request for a copy of their diploma if they have already graduated the high school.

V. Threats & Vulnerabilities

With hundreds of possible vulnerabilities and threats that could damage the IT department's assets, a few examples will be discussed as to how a threat should be studied in an information assurance scenario. For this, an asset will be chosen, and multiple threats will be analyzed for that specific asset. This includes looking at threat agents, threats, vulnerabilities, and the impact that it will have on the confidentiality, integrity, and availability of such specific asset.

A. Online Portal

The first possible typical threat that can happen to an online portal is a system/software update (threat agent) which can cause incompatibility with the online portal if it is not properly maintained (the vulnerability). Old websites tend to lose a lot of functionality if not kept up to date, with their web certificates valid and their requests following the right protocols. If certain functionalities from the online portal are lost, it can completely affect its availability to students and teachers, as they would not be able to access it. The confidentiality, integrity, authentication, and non-repudiation of the data should still be maintained, however, since nothing has happened to the data from the portal.

A second possible threat scenario for the online portal is with the administration or the IT forgetting to renew/pay for its license/domain due to inadequate system planning and acceptance. This would call a complete system shut down and make the entire web portal offline. This would bring the heaviest impact to the availability of the system as, again, students would not be able to access it.

The third scenario that can happen in these cases is to have a student with low training in IT set his/her password to an old password that has already been leaked. This will decrease the integrity of the system as other users with malicious intent and deeper knowledge of how to use the leaked passwords can easily get into the system using that student's leaked password if no system is in place to check if the password created has already been leaked. In this threat, there would also be a confidentiality impact as an unauthorized user would be able to see confidential information from the system. And to a further extent, if the hacker has a malicious intent, they can easily change the password, taking out the availability of the online portal to that specific student.

B. Digital Data

The first threat to be studied for all data assets is a hard drive failure. These failures are common to happen with corporate servers within their lifetimes. When hard drive failures happen, data can get corrupt, or some data loss can also happen. If there are no back-ups done to the database, essential data will be lost, with a major impact on the availability of the data. This will end up with essential school operations from the management and from classes to be cancelled.

For the second threat to the digital data, a student, teacher or staff member can have clicked in a fishing email which are very common to be targeted to schools. These malicious emails can take over the control of the database, completely affecting everything systems related in the school, from the confidentiality and integrity to the availability and authentication. This is because a hacker can gain full control of it if they can get the proper logins and passwords with the phishing emails. This will only happen if there is a lack of training for the staff for this kind of email and lack of controls and malicious software in the school environment.

For the third threat, we can look at a new, untrained teacher who is not familiar with the school's portal. Teachers can easily cause the grades for all the students to be available to everyone instead of just to the individual. This will make the teacher wrongly release confidential information. The vulnerability for this is mostly procedural, as there are no procedures and training in place for the teachers to get accustomed to the school's portal

C. Network Hardware

The network hardware for the schools is also exposed to multiple threats and vulnerabilities. The first threat to be studied is equipment failure due to an energy surge. Energy surges can happen due to multiple reasons, like a power outage or a thunderstorm hitting near the school. However, an equipment failure will only be caused if there is not enough equipment security put in place when building this infrastructure. This equipment includes uninterruptible power supplies or proper circuit breakers. This will mostly impact the availability of the network, since with the equipment offline, the network will be inaccessible.

The second threat is when there is a threat agent that wants to target the school's Wi-Fi. Any user who lives right by the school and is in reach of the school's Wi-Fi signal can access it since the school does not have any passwords protecting the Wi-Fi. This is a huge vulnerability due to the lack of monitoring

systems that look at who is accessing and using the network. This can cause huge problems since the user will instantly break the integrity of the network because there is unauthorized traffic going through. Furthermore, if the user is malicious, it can have an impact in the availability and confidentiality of the network.

VI. Controls

For the controls section of the report, the NIST Special Publication 800-53 is a report which was done with a catalog of security and privacy controls for information systems and organizations. It is made to protect organizational operations and assets as well as other individuals and companies. This is the report that is looked to in order to find appropriate controls to implement in the Infinity High School and reduce the risk of some of the threats mentioned above. More specifically, the systems and communications protection controls will be looked at for the purposes of this report.

The first control to be implemented is to protect the authenticity of communication sessions. This means to protect session authenticity addresses communications at the session level instead of at the packet level. This authenticity will protect the network users from "man in the middle" attacks, session hijacking, and the insertion of false information into sessions. This can be implemented by only allowing the use of TLS 1.3 communication protocols for the firewall instead of allowing older and obsolete protocols to occur.

Continuing to look at the firewall, the boundary protection of denying by default should be added. This will make sure that all random traffic is denied by default, and only allowing by exception. This should be when the firewall is programed to deny everything at first except if the network traffic is one from a specific list, such as having incoming and outgoing mail to the email and web server are only allowed if going from port 443. This is essential to keep the integrity of the network.

Another boundary protection control to be added is to limit the number of external network connections to the system. This means that the access points and the entire infrastructure should be created to only allow a certain number of devices to be connected at the same time. This imposed limit will facilitate the monitoring of inbound and outbound traffic and make sure the firewalls and rest of the network traffic is never overloaded. For this specific case, since the school has around 300 students and around 50 employees, it can be said that no more than 500 devices should be connected to the network at the same time.

In the network topic, wireless link protection controls should also be added. This includes the controls and systems monitoring to ensure no attacks such as the evil twin attack are occurring. These are attacks where the wireless name from the school is doubled in order to have people access it and subsequently, all of their information going through that network is inspected. The control for this is to have constant monitoring for double networks and be immediately shut down if found. A network certificate should also be created, and it is recommended for the Wi-Fi to be immediately secured with a password.

The next control looks at the session authenticity. It should only allow the use of proper certificates, trusted by reliable organizations for the verification of the establishment of protected sessions.

The next control that should be added to the school is aimed to protect the information at rest. This will ensure the integrity of the data by creating back-ups, when necessary, only allowing change of data (like grades) by authorized users, and by creating digital signatures after encryption.

Lastly, it is important to look at cryptographic protection to ensure that all the data held by the school is protected. For this, controls needed to be added to ensure all information recorded in the data, mail, and web servers are encrypted. For this, it is recommended that the school uses an encryption from the AES family and hashing like the SHA-256. This will support both the integrity and confidentiality of the data as, if stolen, it cannot be read and, even if an intruder gets inside the network and servers, they still cannot change the data which is stored inside the servers.

VII. Reccomendations and Costs

Starting with the recommendations for the school's network and infrastructure (IT related), the first recommendation is to install proper firewalls in order to keep the network running safe. Two industry standard firewalls (e.g., Palo Alto Networks Firewall PA-850) should be able to handle 500-600 users at the same time. It is recommended that these networks are properly configured (by blocking everything and only allowing exceptions). This will ensure the safety of the network. As for the cost for these firewalls, it should have a total cost between $12,000 and $15,000. This is done to prevent any network attack as seen in the threats for the network hardware.

The second recommendation for the network's infrastructure is the installation of UPS systems. This will provide protection from power surges to any device such as switches, gateways, and firewalls. This will protect the higher cost devices while completely eliminating the threat of a power surge as seen in the network hardware section of the possible threats and vulnerabilities.

The third and final major recommendation for the network's infrastructure is to install a mesh wireless solution which is password protected. This recommendation will ensure that no unauthorized and unauthenticated users can get in and use the school's network. The total cost of the installation will be anywhere between $28,000 - $30,000, assuming all equipment is commercial grade. An estimate breakdown of the costs for the mesh network installation is listed below in table 1.

TABLE 1: COST BREAKDOWN FOR MESH NETWORK HARDWARE

Equipment	Price	Quantity	Total Price
Wifi Access Points (Cisco Catalyst Access Point)	$1,495	12	$19,940
Wireless Network Controller (Cisco Catalyst 9800-L)	$7,500	1	7,500
Wiring	$170	500 ft x 2-3	$500
Installation	$500	1	$500
Internet connection	$500	1 (monthly)	$500
Total			**$28,000 – 30,000**

VIII. CONCLUSION

To conclude, when looking at all assets in a high school from its technology sector, different vulnerabilities and threats are studied. To ensure these vulnerabilities are dealt with, some controls and recommendations were presented along with the costs to put such recommendations in place. With all these recommendations, it is useful to keep looking at many other possible vulnerabilities which can then occur. For example, having firewalls and wireless network controllers in place in the school also increase the risks of theft in the school since valuable material will be stored in the school, therefore some physical controls would need to be put into place. This will happen to every single control and recommendation that is put into place, since these open up new vulnerabilities into the school environment.

Furthermore, some new controls and recommendations can and should be looked into. Controls such as back ups are very important for the data security side. Other controls to ensure that the personnel work correctly with the students' data should also be studied to ensure that FERPA laws are followed with the school.