Education: Security Challenges

Introduction

Why is higher education becoming one of the most popular targets for cyberattacks? Let’s take a look at the facts.

High schools and Universities have relatively open networks. These open networks contain very extensive qualities of sensitive student data. Any given university has a huge wireless network that connects every office, dorm, classroom, and building to the same wireless connection. Although very strong with multiple bandwidths, this ‘multiple’ network highway that leads to one exit which contains the privatized student data such as payment information, social security number, addresses, etc. Additionally, higher education must comply with many different laws to protect student data. The requirements of these laws may indirectly restrict the IT infrastructure of the institution or open it up to hackers.

Challenges in Higher Education

Blackstratus is a software company that focuses on managed security services by creating solutions that automatically comply to the current laws. Their article, “Higher Education: Compliance, Security and Data Logging Standards” mentions the challenges that higher education institutions face when exposed to cyberattacks.

Higher Education is facing threats because the industry and its surroundings are changing. As time passes, society is pushing toward a technological environment. More people are buying the latest editions of phones, tablets and laptops, and as a result, society is beginning to push the use of eBooks as opposed to traditional textbooks.

However, with inexperienced users coming into technology in a rapid motion, many of them could unintentionally expose information without realizing it. An inexperienced user may struggle with newer technologies and can potentially be subject to scams, spoofing, and phishing. These potential threats include hackers messaging for personal information and blackmailing victims for money. Threats from higher education focus on personal information and intellectual property. For example, a cybercriminal could steal information from a student, and they threaten the student for money or else they sell that student’s information. Another example is a cybercriminal could focus on a wealthy student, threatening the university with stealing thousands of pieces of information in exchange for that one student’s information (social security number, financial information, et cetera).

Biometrics will be the strongest defense against cyber-attacks in higher education. Stop using passwords and start using your fingerprint.

As mentioned before, the network around a university or a high school allows hackers to swiftly enter and exit a system without being detected while leaving detrimental damage. Educational institutions tend to keep everything under one roof to establish an open network architecture with multiple access points. Due to this, if someone misplaced their cellular phone, for example, a malicious person could potentially log into the system and access the entire mainframe. Additionally, students working in a technological office also have access to wireless connections which means that if the victim works in one of these offices, the hacker could have access to login information such as where and when students accessed the wireless network.

Data Security Solutions

Thales eSecurity is a company focusing on SaaS solutions in cloud and data security. Their article "Data Security Solutions for Educational Institutions" focuses on the higher educational side of problems and how to solve for them. The organization focuses on securing sensitive data. In an institution, knowledge is obviously the largest focus, but because an institution cannot 'file' knowledge into a system, they file report cards based on exams and classes. The following data is formatted to be filing into the server.

First, intellectual property from the government and privately funded research are sets of information that, if stolen, could cost the institution a large amount of money. Intellectual property refers to patents or documented permission from the government. For example, a nutrition-based research project must use human subjects to test the dietary aspects of their product. Because of the human-related research, the project team requires an Institutional Review Board (IRB) which is an FDA group that provides documented permission to test on human subjects if approved. However, if a hacker was able to steal this information and revoke the IRB, then the project team is now open to a potential lawsuit in the case of safety or if a failed experiment occurs.

Second, faculty and student personal identification is available (if you look deep into the server). This information includes healthcare, credit card/payment options especially from paying the semester's tuition, and other light information such as classes and majors. Besides this, students and all staff/faculty have their employment information such as direct deposit bank accounts or addresses if the paycheck is mailed. This data is highly sensitive and if targeted would be negative for the victim.

Lastly, institutions are required to comply with regulations and standards laid out by the surrounding environment and the laws of the country. There are many government regulations that the higher education institution is required to follow, but in doing so they leave themselves open to a potential attack that they are unable to stop because of the regulations. The Family Educational Rights and Privacy Act (FERPA) has a singular purpose: to ensure the privacy and protection of education records and the only one who can access these records is the “eligible” student. Another regulation is Payment Card Industry Data Security Standard (PCI DSS) which requires the institution to accept major credit card organizations such as American Express or Visa. Additionally, the combination of Health Insurance Portability and Accountability Act and Health Information Technology for Economical and Clinical Health regulations (HIPAA-HITECH). HIPAA protects a patient’s data from being transferred from one location to another during the process of moving from location to location, school to school, and workplace to workplace. For example, a student transferring into a new university must provide health-related data such as current health insurance or applying for the university’s health insurance. Then, this data is going to be protected under the HIPAA regulation until the student is completely transferred into the new school. HITECH simply promotes the usage of health information technology, and current students are exposed to this because current students must provide health information through the university’s website.

Cyberattacks History in Higher Education

Cyberattacks are not a recent phenomenon. In fact, they have occurred several times over the past two decades. The first instance of cybercriminals in higher education occurred at Yale in 2002. In 2002, Yale University was hacked by students from Princeton University because Princeton wanted information on admission decisions which means that Princeton stole records of students’ and staff members’ personal sets of information. In 2004, two million records from various California universities were stolen, including 800,000 records from the University of California – Los Angeles.

Personal data is the main target for all these attacks. In June 2005, the University of Hawaii was targeted and had personal data stolen of 150,000 students. Sometime after this attack, the University of Utah had 100,000 names and matching social security numbers of former employees from a librarian who formerly worked there. In 2008, personal data was the focus of information. This has become worse over time as the 70,000 records that were originally stolen have now become 700,000 records.

How Biometrics Can Help

Once a problem is internal, it might be too late. This means that the best defense must be from the outside to prevent any cyber-attacks from reaching the inside. Biometric technology is beginning to become less of a luxury and more of a quick, convenient, and highly secure option of logging into a system. Fingerprint authentication relies on a highly unique set of identification that will always be on 'the tip of your finger'. Instead of using a passcode that many people can remember, only one person can log into a cellphone using a fingerprint or face identification.

Within the sector of education, students can start using their fingerprint as their credentials. It is more convenient because:

1. The authentication rarely fails.
2. If you forget your password, you need reset your password, thus making a difficult string of characters that you must memorize.
3. You cannot 'forget' your fingerprint.
4. Typing a twelve-character password takes more time compared to waiting a second for your device to recognize your fingerprint.

Additionally, it becomes safer to use biometrics because a student cannot 'lose' or transfer their face or fingerprint. Those will always stay with the user. As well, if a cybercriminal steals a laptop that utilizes biometric technology to log in, then the cybercriminal cannot pass the login screen.

By having all students establish fingerprint authentication, not only can biometrics protect the network architecture, but also every dorm/apartment can require fingerprint access. Because most dorms require a student to swipe their ID, if the student forgets their identification, they do not have to worry as they always have their fingerprint.

Biometrics is becoming one of the most secure ways of protecting information, and from here on, biometric technology will be involved. There will no longer be a time where biometrics are not relevant in securing student data.

After all, current biometric solutions allow users to use their fingerprint to log into cloud services such as Dropbox and OneDrive. Additionally, Apple's current iOS update allows users to save their password for any service. Then, the user can use their fingerprint or face identification instead of inputting their saved password.

Biometric solutions such as BIO-key are currently implementing fingerprint readers to help protect educational institutions. BIO-key has already partnered with other biometric companies to provide a safer solution when experiencing chaotic emergencies through its incredible data point recognition system.

Biometrics are going to be the strongest defense against cyber-attacks in any scenario including higher education. The best way to help is to stop using passwords and start using your fingerprint.

https://www.blackstratus.com/industries/higher-education/
https://www.thalesesecurity.com/solutions/industry/education
https://www.informationsecuritybuzz.com/articles/cyber-attacks-history-in-higher-education/