Project Milestone 1

ISQS 5342 Big Data Security

Texas Tech University

04/07/2024

Emily Spector

James Parker

Jonathan Busch

Contents

[Part 1 – Introduction and Industry Background 3](#_Toc163160048)

[Part 2 – Relevant Threat Trends and Critical Asset Identification 4](#_Toc163160049)

[Relevant Threat Trends 4](#_Toc163160050)

[Identify critical assets 5](#_Toc163160051)

[Part 3 – Threat Scenarios 7](#_Toc163160052)

[LMS – Injection Attacks 7](#_Toc163160053)

[University-Main Website – DoS Attack 8](#_Toc163160054)

[Personal Devices – Social Engineering 8](#_Toc163160055)

[Wireless Networks – Man-in-the-Middle (MitM) Attacks 9](#_Toc163160056)

[Productivity Software Suites – Phishing 9](#_Toc163160057)

[Part 4 – Intelligence Buy-In 10](#_Toc163160058)

[Part 5 – Group Roles and Signatures 11](#_Toc163160059)

# Part 1 – Introduction and Industry Background

The industry we have chosen for this project is that of higher education. The key services that higher education provides include degree programs, research, and student services. Degree programs contain any service related to courses, accreditation, educational materials, and labs. Research refers to activities that can be published in academic journals. Therefore, services related to procuring the ability to perform this research are related to this service. Finally, the last identifiable major service within education is student services. This refers to activities that provide students with food, dormitories, doctor visits, tutoring, and other miscellaneous services related to students.

Education takes up a sizable chunk of the U.S. economy with 6.4% of the U.S. GDP spent on education from both private and public sources in 2020. The spending on education as a % of GDP has decreased by 16.7% within the period of 2010-2020. There are approximately 11.51 million students (about twice the population of Arizona) enrolled in higher education in 2023. The US department of education found 4000 degree granting academic institutions. Due to the 2020 pandemic, online education, which includes non-degree granting institutions, has grown significantly with the total number of registered online learners on Coursera alone reaching 92 million users.

The major industry players in education include the Federal Government, State Government, Donors, and various Private Institutions. Federal and state governments act as a source of funding for public institutions such as Texas Tech. Donors will spend money on schools for specific purposes. Private institutions such as Harvard make up the most prestigious universities.

Information technology has grown to be an important aspect of education. Databases are used to hold student data like grades, identifying information, classes/schedules, and contact information. Furthermore, valuable research information can be held within university databases. This can include in progress research papers and experimental data. Both the student data and research data are targets for cyberattacks due to their value so keeping this information secure is a must.

# Part 2 – Relevant Threat Trends and Critical Asset Identification

## Relevant Threat Trends

The education industry is increasingly reliant on technology to facilitate learning, research, and administrative functions. However, this dependence on technology has made educational institutions appealing targets for cybercriminals targeting sensitive data and systems.

Ransomware attacks are one of the education industry’s biggest concerns. The industry is the second most targeted sector for ransomware attacks, where hackers will encrypt academic databases and financial systems. Credential theft is another significant threat, compromising login credentials of those associated with the institution and exposing individuals to identity theft and fraud. Phishing attacks remain prevalent, exploiting human vulnerabilities to compromise networks and steal valuable data.

Prime targets from these institutions for cybercriminals are academic databases and intellectual property, such as research. Educational institutions are continuing to adopt new technologies, which include learning management systems, cloud services, and Microsoft Suite. While these technologies are essential to modern education, they also introduce additional vulnerabilities and require institutions to implement more advanced cybersecurity protocols.

Key people targeting this industry come from many different backgrounds and have many different goals. There are cybercriminals looking for financial gain, utilizing a ransomware attack, for example. Such an example of this is when Cl0p Ransomware, a Russian-speaking ransomware gang, hacked into a third-party software tool known as MOVEit, which effected over 890 universities. Government-sponsored entities engage in cyber threats against educational institutions with the goal of gathering research data and intellectual property, while Hacktivist groups target educational organizations and may conduct DDoS attacks to contribute to online activism and digital protesting. Even insiders, including students, faculty, staff, and contractors, pose significant cybersecurity risks to educational institutions. Insider threats may involve malicious actions, such as data theft, sabotage, or unauthorized access, driven by financial incentives or personal grievances. Additionally, unintentional insider threats, resulting from a combination of negligence, human error, or lack of cybersecurity awareness, can lead to accidental data breaches and security incidents because of negligence and insufficient training on cybersecurity.

## Identify critical assets

Five of the most critical assets that Higher education relies on include Learning Management Systems, primary university websites, personal devices connected to university networks, the university networks themselves, and productivity software suites.

Learning Management Systems (LMS) act as portal for a large amount of university activities. Two examples of these systems include Canvas and Blackboard. These allow the uploading of notes and videos, a place to turn in assignments, ask questions online, and access/modify grades. Many classes rely on these systems and would have to make drastic changes to operate without them. With these systems down, students cannot turn in assignments, access grades, and communicate within the system. Professors will be unable to upload notes, add/change grades, and create supplemental content. Online classes that entirely rely on these systems will be unable to function in their entirety.

The University Main Website is used for more administrative tasks within the University. An example of this would be Raiderlink used by Texas Tech University. This system allows users such as students, professors, and faculty to schedule classes, obtain transcripts, and enter hours worked. If this system were to fail, there would no longer be easy access to these services. Furthermore, the database that holds this information contains critical information on students and faculty and having this information leaked could cause major financial damage to the victims. This would also incur major reputational damage to the university as people would be less trusting in giving up personal information to that university. A major breach could cause more regulation in terms of storing student information in which staying compliant with these regulations could be potentially costly.

Personal devices are used for many classes and activities within the university. These devices allow students and faculty to perform tasks that would be possible without them. This could include performing in class assignments to digitally record research information. If these devices were to be attacked the university would incur both reputational and financial damage. Many would feel unsafe using their personal devices post breach thus lessening future enrollment and damaging research functions.

Wireless networks are a critical asset for universities and higher education institutions, as they are vital for connectivity across campuses. Students, faculty, and staff rely heavily on these networks to access essential classroom tools, communication platforms, research resources, and online learning platforms. For example, learning management systems (LMS) and educational applications rely on WIFI connections to enable remote or online learning, collaboration, and information sharing. The consequences of a breach or compromise of these critical assets can be severe. Such incidents could disrupt classes, compromise sensitive data, undermine academic integrity, and disrupt institutional operations. Students, faculty, researchers, administrative staff, and visitors are the primary users of these assets, highlighting the broad impact and significance of maintaining the security and reliability of wireless networks in higher education settings.

Institutions of higher education heavily rely on productivity software suites like Microsoft Office, Google Drive, or any service like these. These services are used by all faculty, staff, and students for efficient document creation, collaboration, cloud storage, and accessibility to educational resources. A breach of these critical assets could lead to data manipulation, disruption of service, reputation damage, and compliance issues, impacting operational efficiency and trust among stakeholders (students, etc.). Protecting these assets from cyberattacks is crucial to safeguarding sensitive data, maintaining continuity, and upholding regulatory compliance within higher education institutions.

# Part 3 – Threat Scenarios

In this section, we will discuss some possible threat scenarios within the industry of higher education. Parts of these scenarios will be modeled after the current threat trends in the industry, as discussed in an earlier section. For example, some of the adversaries described in these scenarios will be cybercriminal organizations, reflecting the Cl0p attacks that affected several universities.

## LMS – Injection Attacks

Adversary: Current student or students at a university trying to gather data of their classmates.

Capabilities: SQL-Injection, Cross-Site-Scripting Vulnerabilities.

Infrastructure: The LMS itself. Injection attacks directly exploit vulnerabilities in websites or applications without needing external networks or assets. Attackers inject malicious code into input fields, manipulating functionality to compromise data or execute unauthorized commands within the system itself.

Victim: Not only the university the student attends. All universities using the LMS would be put at risk. Therefore, every student at each of these universities could possibly be the victims.

## University-Main Website – DoS Attack

Adversary: Cybercriminal organization wishing to do harm through a DoS attack.

Capabilities: In this scenario, the adversary may have access to networks of compromised devices that can generate a massive volume of traffic directed at the university's website. It would also be possible that the adversary was well versed in the websites infrastructure to best exploit and overwhelm it.

Infrastructure: The primary infrastructure in this case would be the compromised devices, which could be computers, IoT devices, or the adversaries command and control servers.

Victim: The students, faculty, and staff of the university (and all “legitimate users” of the website) would be the victims in this scenario. These parties would not be able to access the website or its services.

## Personal Devices – Social Engineering

Adversary: Student gaining access to another student’s personal device with the goal of impersonating them to get sensitive information.

Capabilities: The adversary would have knowledge of social engineering techniques, phishing skills, or could possibly be informed on malware development and deployment.

Infrastructure: The infrastructure would be the adversary's communication channels, such as email, phone calls, social media, or in-person interactions, used to establish contact with potential victims.

Victim: The person whose device was compromised. By extension, the institution would also be at risk, especially if the individual victim was a person of high stature or importance (a president of a university for example).

## Wireless Networks – Man-in-the-Middle (MitM) Attacks

Adversary: Cybercriminal Organization trying to gain access to sensitive information, gain unauthorized access, or disrupt network communications.

Capabilities: The adversary possesses knowledge and tools for conducting MitM attacks, such as ARP spoofing, DNS spoofing, SSL/TLS stripping, or Wi-Fi Pineapple devices.

Infrastructure: The infrastructure in this case would of course include the wireless network that the adversary is accessing, along with the adversaries “attack tools,” such as Ettercap.

Victim: The victim in this scenario would be any person (student/staff/faculty/etc.) connected to the wireless network.

## Productivity Software Suites – Phishing

Adversary: A cybercriminal organization specializing in identity theft and email-compromising schemes.

Capabilities: Targeted phishing campaigns to trick users into revealing their Microsoft login credentials, enabling unauthorized access to email accounts and sensitive documents.

Infrastructure: The adversary operates from temporary email addresses, compromised websites, and phishing landing pages designed to mimic legitimate Microsoft login portals.

Victim: Students, faculty, and administrative staff using Microsoft Suite services for email communication, document collaboration, and administrative tasks

# Part 4 – Intelligence Buy-In

The landscape of cybersecurity in the education sector is an ongoing challenge that is constantly evolving. Current threats are phishing attacks, ransomware, insider threats, data theft, and DoS attacks. Higher education institutions experience security breaches relatively frequently, and with a concerning 20% increase in breaches from 2022 to 2023. With the growing use of technology and cloud services, we expect this threat to continue to be an even larger issue.

To combat these challenges, universities are investing in educational initiatives aimed at faculty, staff, and students to promote knowledge about cybersecurity practices, along with implementing stronger cybersecurity protocols to help prevent incidents and stay informed about emerging threats.

The cost of a data breach is substantial; universities must cover remediation costs, legal fees associated data protection regulations, and the loss of valuable intellectual property. On average, universities end up facing a financial burden of $3.65 million per breach.

Utilizing intelligence-based security can alleviate these financial strains. By facilitating early detection, rapid response, and proactive risk management protocols, universities can have a strong defense against cyberthreats. This will not only minimize the impact of breaches, but also will ultimately reduce the financial costs associated with them.

# Part 5 – Group Roles and Signatures

James – worked on part 2 and part 3 (33% of total work)

Jonathan – worked on part 1 and part 2(33% of total work)

Emily – worked on part 2 and part 4 (33% of total work)