Gabriel Hervias
2452 Canyon Circle
San Luis Obispo, CA 93410

IT Cybersecurity Representative
Cal Poly Information Security Department
1 Grand Avenue
San Luis Obispo, CA 93407

June 3, 2021

Dear ITS Cybersecurity Representative:

As a group project for English 149 Technical Writing for Engineers, my group and I are enclosing a report about cybersecurity and data breaches in higher education institutions and in the financial sector. The audience of this report consists of people who are affiliated with higher education institutions and the financial sector. The group consists of three first year computer science majors at California Polytechnic State University, San Luis Obispo.

When researching, the group used library resources and contacted cybersecurity professionals involved in the education and financial sectors. Through these resources, we found that the software of an institution is a factor as well as the culture of the institution are big roles that play into the effectiveness of cybersecurity. We recommend that people affiliated with higher education institutions and the financial sector should understand the general idea of what cybersecurity is and taking action to protect oneself against cybercriminals. We also recommend understanding the cybersecurity policies and procedures are put in place in their institution.

Outside of the members of our group, Jacquelyn Campbell, our professor, and Doug Lomsdalen, the Information Security Officer for Cal Poly, were instrumental to the creation of this report. Amey Patne (MEng. Cybersecurity, University of Maryland), helped us identify the effects of cyberattacks and gave valuable inputs about technologies used to combat the same.

We are asking you to review the information and provide our report with constructive criticism. If there is any way that you could help us to distribute this report with the purpose of educated our intended audience, that would be greatly appreciated. If you have any questions, please contact us.

Sincerely,
Gabriel Hervias

Gabriel Hervias
Computer Science Student
Cal Poly SLO
ghervias@calpoly.edu

An Analysis of Cybersecurity in Higher Education Institutions and the Finance Sector

Elissa Covarrubias, Ananya Desai, and Gabriel Hervias
California Polytechnic University, San Luis Obispo
June 3, 2021

Abstract

This report analyzes the state of cybersecurity within higher education institutions as well as the financial sector. After performing literature research using the Cal Poly Library's online database, the researchers surveyed the target audience about their experiences with cybersecurity threats and conducted an email interview with a cybersecurity professional.

While studying the intricacies of higher education cybersecurity, it was found that end-user error and hacking were the main causes of data breach events. Maintaining awareness of safe cybersecurity practices and common exploits can be extremely effective in stopping these attacks.

There is also a need to understand cybersecurity to be part of the defense against cybercriminals and data breaches. A person aware of cybersecurity and the policies put in place by their institutions is a positive step towards building a culture of cybersecurity awareness and lead other to understand the importance of cybersecurity.

Our finding of cybersecurity in the financial sector concludes that the financial sector is one of the sectors most vulnerable to cyberattacks. Effective technologies are being developed to counter these attacks and financial institutions need to keep themselves updated with the same. It is equally important for these organizations to train employees and create awareness among end users about the implications of cyberattacks and ways to tackle the same.

A methodical approach to counter cyberattacks by different sectors of an institution is described.

The data breach information from the Privacy Rights Clearinghouse database shows downward trends in the number of data breaches in both the education and financial sectors. Irregular year-to-year changes are attributed to a continuously evolving cybercrime environment.

Key Terms
education, financial, data breaches, cybersecurity, analysis, culture, vulnerability, trends

Table of Contents

List of Illustrations

1.0 Introduction

As more and more parts of our lives move online, more of our valuable information is being stored digitally. This includes the information that we give over to higher education institutions and the financial sector, which most people are involved in during at least one point in their lifetime. These institutions are crucial parts of society and economy. The education and financial sectors are big industries, employing thousands of people across the globe. Because of how large these sectors are and the amount of valuable information they handle, they are targeted heavily by cybercrime. The cost for institutions after a **data breach*** could cost thousands or millions of dollars. This was the case for Maricopa County Community College District where the data breach between 2009 and 2001 cost the district $20 million (Beaudin, 2015). That is why it is crucial to understand how cybersecurity works in the educational and financial sectors. After all, if we spend much of our time in educational systems and are dependent on the financial sector, then we should try to understand how cybersecurity works in these sectors.

1.1 Cybersecurity

Cybersecurity, in the most general terms, is the protection of digital and online **assets** within an organization. Cybersecurity ensures the confidentiality, availability, and integrity of these assets. These are the three main principles of cybersecurity. However, the specific security concerns and policy requirements of an organization are ultimately what determine how a system should be secured (Bishop, 2003). The number of people involved in an organization, the type of information shared, and the operating systems of the hardware used are all factors in the computing environment that an IT team must take into consideration. An organization's approach to cybersecurity is done by risk assessment, which typically has the initial step of identifying assets, threats, and vulnerabilities (Ulven & Wangen, 2021).

Assets are either information or business processes considered valuable by an organization. An organization's assets can come in many forms. They can consist of things like passwords, credit card information, and health records. These types of information are usually what is thought regarding cybersecurity. However, assets include things like, computing power, communication systems, company schedules, and websites. As you can see, assets do not only consist of private information. Additionally, some assets are required to be available to certain groups, or even the general public. Cybersecurity practices maintain that the correct assets are available to the correct groups. Cybersecurity attacks tend to target the more valuable assets within an organization. Sometimes, certain assets are obtained with the intention of obtaining further assets. For example, the login information of administrators within an organization can be targeted with the intention of accessing **Threats** are potential instances or causes for harm to an organization. A threat may be a state actor, a cyberterrorist, a disgruntled staff member, or a hacker who is simply testing their abilities. Threats, or threat agents, of all forms have the potential to harm the assets of an organization. A **vulnerability** is a specific weakness within an organization's attack space. A system can have many different types of vulnerabilities within its attack space, all varying in complexity. For example, an employee leaving their work laptop in a public restaurant can be just as devastating of a vulnerability as can a lack of encryption of customer financial data. These three aspects of risk assessment are meant to protect against threat events, which often come in the form of data breaches, where data valuable to an organization is leaked, destroyed, manipulated, or stolen.

*This and all subsequent bold-faced terms are in the Glossary on page 23.

2.0 Cybersecurity in Higher Education Institutions

As discussed in the previous section, different industries have unique computing environments that tend towards certain threat events. Higher education institutions have a few main characteristics that set them apart from other industries. In this section, we will discuss the assets typical of **HEI** (Higher Education Institutions), unique elements of HEI cybersecurity that separate it from other industries, and the main threat events that occur in HEI.

2.1 Assets in Higher Education Institutions

Universities and colleges are not simply educational institutions. There are a wide variety of operations that universities, especially larger ones, oversee. According to a white paper by James, Dominic, and Paluzzi (2016), HEI are financial institutions, medical institutions, and retail establishments. Through these institutions, data is collected from donors, trustees, board members, alumni, students, parents, applicants, faculty, staff, medical patients, consumers, and vendors. Because of the variety of these operations, universities have many assets. These can include student records, research data, financial information, health records, on campus high performance computers, etc. Table 1. Proposition of the most valuable information assets by KPI shows these assets as sorted by Key Performance Indicators (KPI), which is defined as "a measurable value which explains the effectiveness of an institution and how it is achieving key objectives" (Ulven & Wangen, 2021).

Table 1. Proposition of the most valuable information assets based on KPI

KPI	CRITICAL INFORMATION ASSETS
ENROLLMENT & GRADUATION	Student PII and records
	Learning and teaching information
	Financial management information
STAKEHOLDER SATISFACTION	Sensitive Research information/data and IP
	Government and Third-party data
EMPLOYEE & HR	Employee & Student PII
	Administration details
	User and administrator accounts
IT SUPPORTING SERVICES	Bandwidth and Internet Connection
	Computing power and resources
	Communication systems and data

Source: Adapted from Ulven, J. B., and Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), 39.

Certain assets are required to be available to only students and staff, some to high-level administrators, and some to the general public. For example, the results of a study held at a university may be accessed by the public through a university's website, while access to a university's library database can only be accessed by students and teachers. Typically, an attacker will access resources with the goal of financial gain. However, there are other less common attacker motives that are unique to university assets. Research programs with sensitive contents, such as government-contracted studies, can be a target for threat agents looking to compete in some way

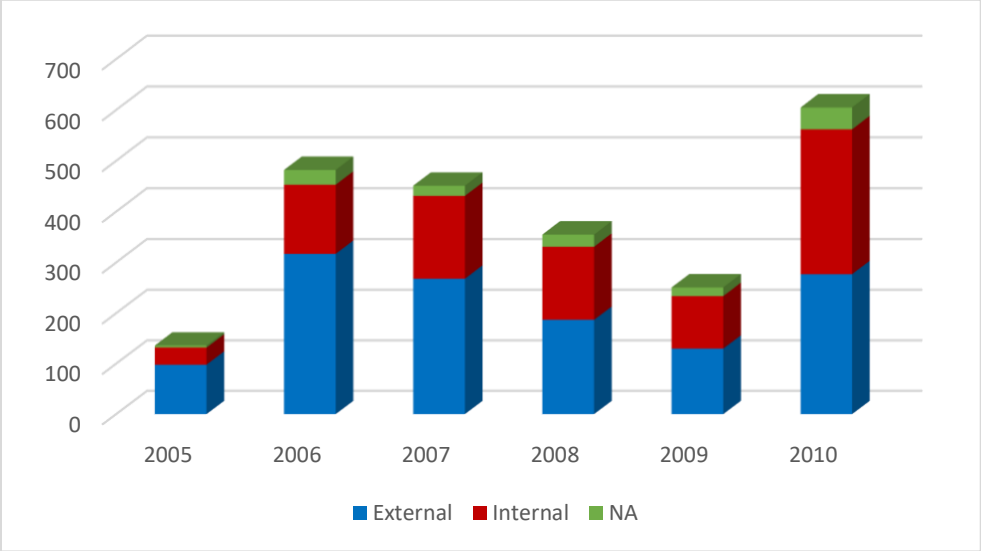
with their sponsoring government or associated state-owned companies. Other motives can be political, where an attacker has the goal of protesting a university in some way by defacing a webpage, for example. Accessing private information from a university and releasing it to the public is another way an attacker can disrupt a university for political purposes (FireEye, 2016)

2.2 Differences between HEI and Other Industries

The information security departments of universities face a couple of challenges that are not typically seen in other industries. Every year, new students are added to a list of members who have access to resources within a university. Graduating students are removed from this list. A constant rotation of access restrictions on top of the typical flow of employees is routine in HEI. Additionally, universities tend to have many students and staff. Effectively securing a network like this is very difficult for administrators (FireEye, 2016). Academia in the U.S. is typically seen as having values of openness and availability of information with regards to research (Ulven & Wangen, 2021). These values are almost opposite to those of cybersecurity. From a cybersecurity perspective, unnecessary access to assets is ideal, as it reduces the potential points of vulnerability. Additionally, responses to data breach incidents may be handled differently by HEI than traditional industry institutions. Because of this value of openness, sharing details to students and staff about a possible data breach right away may be a priority for universities (James et al., 2016). This is not always the best course of action when dealing with a data breach event, however.

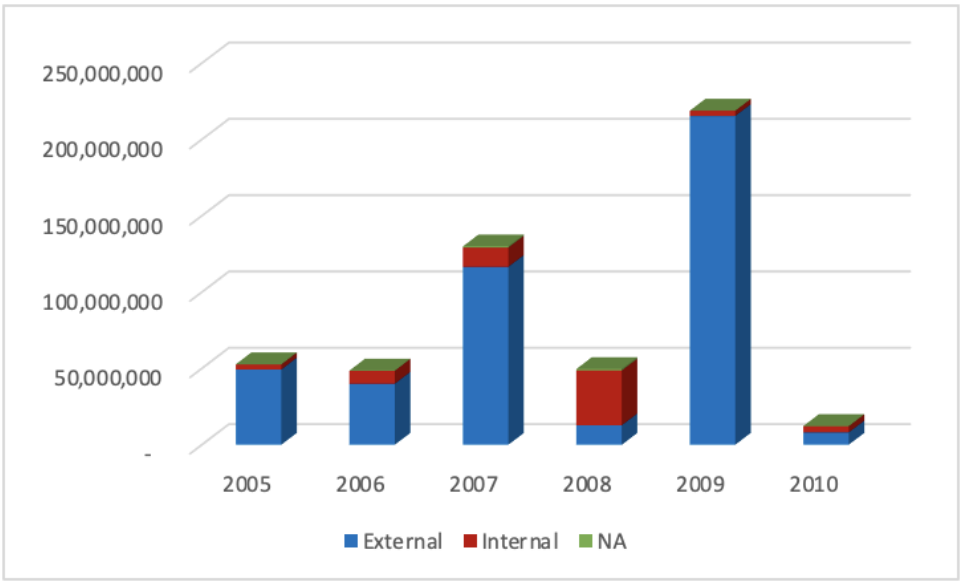
2.3 Cybersecurity Threat Events in HEI

In a study focusing on data breach trends across all industries, Holtfreter and Harrington (2016) place data breach statistics into two main categories: internal and external. **"External" data breaches** are ones involving a third party that compromises data. These data breaches can be both accidental and fraudulent. **"Internal" data breaches** involve data breaches where an employee or member of the organization compromises data. The information that is stolen can be specifically targeted or obtained in some other way. In this article, it is found that 56% of breaches are external, while 37% are internal. Figure A. Data breach trends by number of data breaches shows data breach statistics from 2005-2010, sorted by type of breach.



	2005	2006	2007	2008	2009	2010
EXTERNAL	98	317	268	187	130	277
INTERNAL	34	136	163	144	104	285
NA	4	29	20	24	17	43

Figure A. Data breach trends by number of data breaches
Source: Adapted from Holtfreter, R.E., & Harrington A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, 22(2), 242-260.



	2005	2006	2007	2008	2009	2010
EXTERNAL	49,286,177	39,947,802	116,498,665	12,788,306	215,377,069	8,046,390
INTERNAL	3,282,643	8,461,499	12,638,476	35,802,620	3,410,262	4,075,374
NA	252,790	197,876	828,540	1,068,529	106,084	219,918

Figure B. Data breach trends by number of compromised records
Source: Adapted from Holtfreter, R.E., & Harrington A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, 22(2), 242-260.

This is somewhat misleading, however. These percentages reflect the number of breaches, but not the severity of each breach. The same study found that 86% of records compromised in a data breach were associated with external breaches, while only 13% were associated with internal breaches. These findings are seen in Figure B. Data breach trends by number of compromised records, which shows data breach statistics from 2005-2010, this time sorted by number of compromised records. From comparing these two statistics, it seems clear that external breaches are more severe. The main threat agents across all industries belong to organized crime (Verizon, 2021). This could be the reason why external threats are much more potent.

Verizon's annual data breach report (2021) also finds that 80% of data breaches in education services are external, while 20% are internal. Applying the conclusions from Holtfreter et al. (2015), it appears that external data breaches are much more of a problem in HEI than other industries. The main data breach events that occur in universities are system intrusion and **social engineering attacks**. (Verizon, 2021). **System intrusion attacks** are defined as "unauthorized remote compute break-ins," and social engineering attacks, which are events where a user is tricked into leaking information (Ulven & Wangen, 2021). These two types of events are the some of the most common across most industries.

In a report on social engineering attacks across all industries, Coffey (2016) found that end user error is a root cause of data breaches. In HEI specifically, these social engineering attacks are even more prevalent. This can be attributed to the characteristics of HEI as described in the previous section. Social engineering attacks mainly consist of phishing events, which are commonly seen through email, where an attacker tricks a user into giving out their login information, security questions answers, or other types of information that would give an attacker illegitimate access to a university's network.

System intrusion events such as hacking, malware, and ransomware are the second most common type of data breach event in HEI. The majority of vulnerabilities associated with these attacks are configuration-based errors (Verizon, 2021). Configuration-based errors stem from errors in the configuration of certain programs or services by administrators (Kuhn, Raunak, and Kacker, 2017). According to the 2021 EDUCAUSE Horizon Report, higher education institutional services and data are becoming increasingly cloud-based rather than campus-based. This increase blurs the endpoints of university networks as third-party companies are contracted to provide digital services for HEI, leaving room for configuration-based errors, diminished incident response control and increased incident response times (EDUCAUSE, 2021).

3.0 Cybersecurity Culture and Effects on HEI

It is not just the firewalls and the responsibility of the ITs to prevent cybercrimes; it is the responsibility of all affiliated peoples to do their part in following the policies put in place to prevent cybercrimes from happening in their institution.

3.1 Cybersecurity Culture of Students

The article, *Mobile learning security concerns from university students' perspectives* gets into the students' perspectives of cybersecurity, explaining the culture of cybersecurity for students. (Joy & Shonola, 2014). Joy and Shonola (2014) surveyed seniors of computer science students at three Higher Education Institutions (HEI) in Nigeria. Although this is specific to HEIs in Nigeria, the information presented, and the results can be applied to other HEIs in the world as cybersecurity issues are present in the world of e-learning.

Joy and Shonola (2014) explained the perceptions of students at HEI on use of mobile devices for learning. Some examples of mobile devices are phones or tablets. They found that above 90% of those surveyed thought that the security on their mobile devices was important or very important as shown in Figure C. How important students consider the security of their mobile devices (Joy & Shonola, 2014). Viruses and malware attacks on mobile devices, and especially in developing countries are common). In any country though, almost every young person has a mobile device and has been affected by their mobile device becoming compromised. The security of mobile devices is important to most people. An interruption from using their device for school can lead to less time spent on their classes.

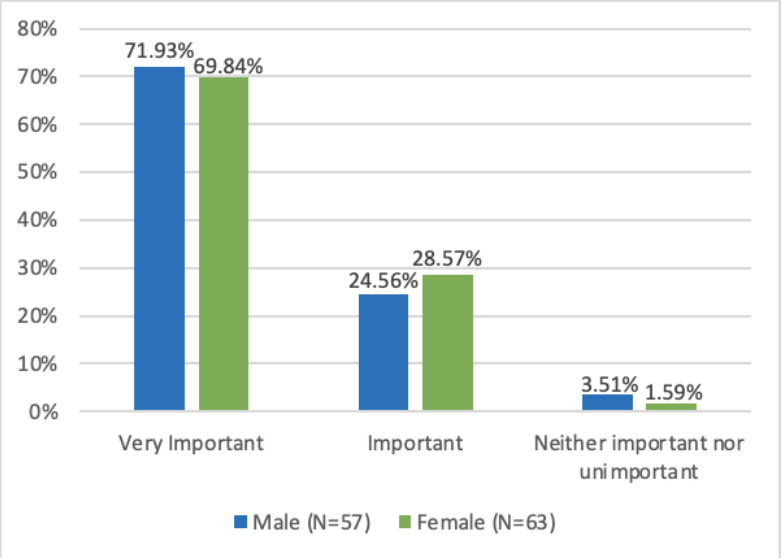


Figure C. How important students consider the security of their mobile devices
Source: Adapted from Joy, M. S. & Shonola, S.A. (2014). Mobile learning security concerns from university students' perspectives. *2014 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL2014)*, 167. Thessaloniki, Greece: IEEE.

Much of the time, learners rely on mobile learning as a complement to the classroom. This is especially true now in a time where there is an increase in reliance of technology in classrooms. Therefore, the need for security in mobile devices is crucial for the learning environment for students and educators. The most harmful effect that Joy and Shonola (2014) found when surveying students about security risks in mobile learning to students, is the loss of their confidential or personal information. This would cause many students would experience physiological disturbance as an effect of their information being leaked. Many students understand the need of cybersecurity and understanding the effects of a data breach. However, it is not just the ability to understand the consequence of data breaches but creating positive behaviors that will help to minimize cybercrime.

3.2 Cybersecurity Culture of Overall HEI

In the article *Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior*, Anwar, Ash, He, Li, Xu, and Yuan (2018) show that when a person fully understands the information security environment and the overall scope of what could happen if a cybercrime were to happen, then they are more likely to follow through on cybersecurity policy and help the overall culture of cybersecurity awareness. The goal of the source is to use **PMT** (protection motivation theory) in an organization to see the current information security behaviors (Anwar et al., 2018). They surveyed 579 business professionals. Anwar et al (2018) wanted to identify the influence of the organization and the action cues from the organization. The influence and action cues from the organization are two main points of PMT. This theory states that the two main points have an influence on the culture of a group. In this study, Anwar et al. (2018) wanted to find out the relationship of PMT influences in the organization and particularly security behaviors. They found that the organization's influence and their response after a cybersecurity breach affected their employees in their perceptions of cybercrimes (Anwar et al., 2018).

Anwar et al. (2018) found that employees' experience of cybersecurity is how they perceive the severity of cybercrimes and vulnerabilities caused by cybercrimes. An example would be that if an organization was affected in a major data breach, the employees at that organization understand from that experience how a cybercrime can impact an organization. This is in contrast with a person who has not been affected by a data breach or cybercrime. The experience from a person affected by a cybercrime understands the full extent of the need for cybersecurity and sees the value in it compared to a person who has not been affected.

The authors also found that peer behavior affected and enhanced actions by fellow employees to take cybersecurity actions (Anwar et al., 2018). Peer behavior leads to a positive culture of cybersecurity and leads employees to become aware of the current measures put in place to fight cybercrimes and breaches.

Being able to have employees aware of their cybersecurity policies will help to execute the policies, resulting in the effort of fighting cybercriminals. An example of people aware of a threat is after the 9/11 attack as the article *Motivating Employees and Organizations to Adopt a Cybersecurity-Focused Culture* explains (Fisher, Porod, & Peterson, 2021). After the 9/11 attack, airports added more security in place. After the experience, people understood the need for extra security at airports and did not complain about how it would take longer to get to their flight. People now, however, complain about the long lines during security checks in airports. This example shows the behavior of people and how an experience affects a person's perceptions. Therefore, much of the time, people will not comply with measures put in place from their organization or an organization does not put

measures in place to proactively stop cyberattacks because they do not perceive or fully understand the risks.

Even though the participants surveyed in Anwar's et al. (2018) study were only business professionals, this can be applied overall to persons affiliated with a HEI. A person's behavior and its effects have a big impact on future cybersecurity threats and the overall culture of an institution. One behavior that many people do not act on is adding security measures in place after being notified of a data breach.

Part of the problem that people need to understand and act on is after receiving a data breach notification. In the article, *Disclosure of personal information under risk of privacy shocks*, from the Journal of Economic Behavior & Organization, experimental study studied how a notification after a data breach affected a person's behavior in disclosing their personal information afterwards (Feri, Giannetti, & Jentzsch, 2016). This was a controlled environment study where they used a person's IQ results as personal data. Feri, Giannetti, and Jentzsch (2016) found that on average, people who were above the median or at the median level would not take much thought after receiving a notification of a data breach. Feri, Giannetti, and Jentzsch (2016) found this group of people were willing to give up some personal information for a discount or incentive. The group of people who were below the median were less likely to give away their personal information but would consider it if they received a greater incentive or discount afterwards (Feri, Giannetti, & Jentzsch, 2016). This experimental study shows that most people who are not in the subcategory of people who see their information as sensitive will not act to protect their PII after receiving a notification of a data breach. This is supported with the surveys Equifax made in 2014 to consumers that fell victim to data breaches as shown in Figure D. How did you respond to the notifications you received in the past two years? In the figure, 32% of the people surveyed ignored data breach notifications they received or did nothing after receiving the notification. It is possible to receive free credit monitoring or pay a monthly fee for credit monitoring. Doing this will help to not being victim to your information being used against you or being exploited. Therefore, it is important to take data breach notifications seriously and act after receiving a data breach notification. Another action to prevent data breaches is understanding the policies of your HEI.

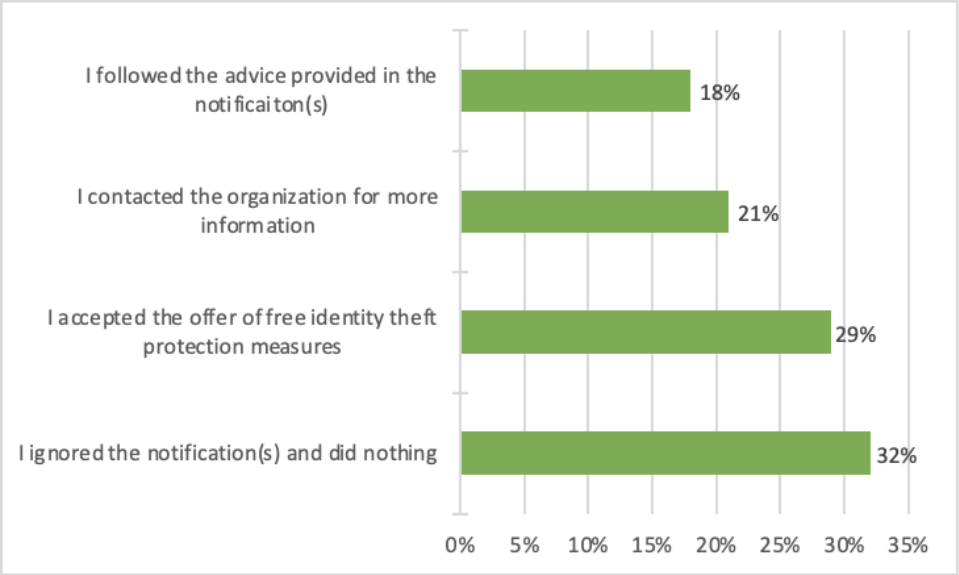


Figure D. How did you respond to the notifications you received in the past two years? Source: Adapted from Ponemon Institute LLC, (2014). *The Aftermath of a data breach: Consumer sentiment.* Sponsored by Experian Data Breach Resolution. Ponemon Institute LLC.

A powerful force against cyberattacks is understanding the policies put in place that are there to prevent cyberattacks and complying to them. Complacency in an organization will only lead to a greater risk of an attack happening as Fisher et al. (2021) point out. The authors talk about creating a culture in an organization that is cybersecurity- focused (Fisher, Porod, & Peterson, 2021). It is important to act before, during, and after an attack to mitigate or minimize cyber risks. A huge part of an organization's vulnerability to a cyberattack is having employees that are unaware of cybersecurity policies put in place or the organization's cybersecurity policies are ineffective or outdated. Fisher et al. (2021) claim that for an organization's policies to be fully implemented, there is a need to change people's behaviors. Reinforcing a person's actions and helping create a cybersecurity focused culture can create a better mechanism to stop attacks from happening. It all starts with your own actions and behaviors that will impact peers around you and move a cybersecurity culture in you HEI.

3.3 Effects of Cybersecurity Data Breaches in HEI

The effects of cybersecurity data breaches on universities and alumni have been a widespread phenomenon. No matter the amount of cybersecurity measures put in place, there are hackers and cyber attackers that exploit the vulnerabilities of their systems. Here are some examples of data breaches that has happened in the last seven years.

3.3.1 University California Irvine (2014)

Hackers infected three computers with a virus that transmitted keyboard input to unauthorized servers. This led to the potentiality of student's PII to be obtained by hackers, although there has been no evidence of that the information has been obtained and used. This may have been caused by unauthorized access. The university provided one year of FraudShop™ credit monitoring and CyberScan™ internet monitoring (California Attorney General, 2014).

3.3.2 College of the Desert Data Security Breach Notification (2014)

An unauthorized employee of the College of the Desert sent an email with an attached spreadsheet containing personal information of employees. This resulted in removing and deleting the email in less than 24 hours from the employees that received the email. The college also worked in examining their protocols to protect the disclosed personal information. This affected 1,900 employees (California Attorney General, 2014).

3.3.3 Wabash College (2015)

A virus was found in an employee's work computer that copied their files on a hard drive. The hard drive was accessible in external servers. The virus encrypted the data, holding the data for ransom. This affected 49 people, 15 of which their social security numbers were compromised (Privacy Rights Clearinghouse, 2020).

3.3.4 University of California (Dec. 2020)

The University of California's Accellion FTA was hacked due to a security vulnerability that affected members affiliated with the UC's. Some PII that were impacted were full names, addresses, telephone numbers, social security numbers, passport information, birthdates, and financial information. In March 2021, they found that some of that information has been posted and leaked onto the internet. They university of California system are providing free credit monitoring and identity theft protection services through Experian IdentityWorks (California Attorney General, 2020).

There have been different reasons for these data breaches and different ways that HEIs have reacted to a data breach. Some had decided to prolong the release of notice of a data breach while others have taken full responsibility on what happened, making changes that will prevent further attacks from happening. In either case, a strong culture of cybersecurity awareness and having behaviors that reflect the policy measures put in place will help to mitigate some cybersecurity attacks. Another important sector that is hit by cyberattacks is in the financial sector. As part of or affiliated with a HEI, the financial sector plays a part in managing the money between you and the HEI.

4.0 Cybersecurity and the Finance Sector

With incessant development in technology, cybersecurity is a recently developed discipline that deals with issues regarding protection of all confidential information about institutions' participants from spiteful digital attacks. As the number of devices over the population increases, the attackers are increasingly improving right now. The frequency and complexity of cyberattacks within financial institutions (regional banks, credit unions, third-party credit providers) are increasing. This could be due to a number of factors, such as the spread of social unrest, strained relations between nations, or extortion.

It has been observed that the financial services sector has been placed in the worst hit industry by cyberattacks for two consecutive years. Across all industries, 27% of security incidents and 17% of attacks were identified in the financial services sector.

Given the intertwined nature of the various sectors within the financial sector, the attack on one part of the institution's infrastructure will have a significant and immediate impact on related areas and the financial sector's vulnerability towards cybercrimes. The financial sector is required to constantly upgrade and monitor their cybersecurity systems in order to maintain the privacy of sensitive information. Consequently, the banking sector has been the dominant field in the administration of security systems.

4.1 Branches of the Finance Sector Affected by Data Breaches

The following are the branches within the financial sector that were identified as platforms where most data breaches have taken place as a part of the analysis of a survey conducted for this report. The survey respondents were people belonging to different age groups ranging from 18 to 65 years belonging to a variety of professions (Figure E. Have you ever experienced violation of your privacy on a digital platform?). Of 137 people surveyed via social media, 66.7% reported that they have faced privacy issues in the past.

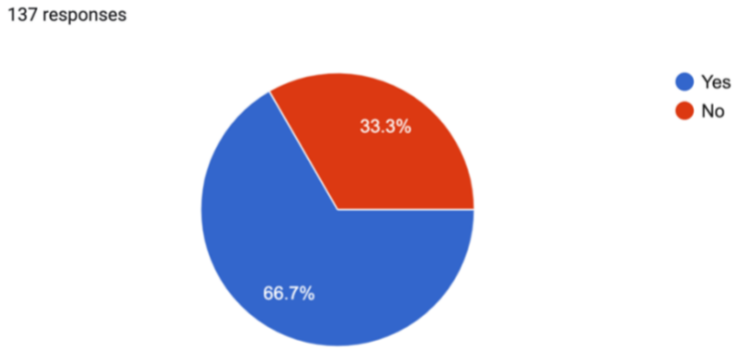


Figure E. Have you ever experienced violation of your privacy on a digital platform?
Source: Author.

4.2 Skeleton of the Data Breach Process in the Financial Sector

This can be mainly classified into 3 steps, viz. Planning, execution and covering tracks. These are elaborated further:

4.2.1 Planning

This is a crucial stage and requires detailed and precise observation of the system. In this stage, the hackers identify the vulnerabilities and loopholes within the system. They do so by observing encryption patterns and try developing decryption technology based on the same framework. They make use of communication channels to collect information about unencrypted data and manipulate it in a way useful to them to carry out the heist. They also collect information about IP addresses and network services used by the organization, which they may potentials use as pathways to access their servers. Using all such information gathered, they make a well-defined layout of how to carry out the heist.

4.2.2 Execution

The vulnerabilities identified in the previous step are now used as a channel to attack the target's system. The possible pathways are identified as follows:

1. Phishing: This is a method where the attackers portray appealing visuals or texts disguised as legitimate methods to lure the users to perform actions to provide sensitive data.

2. Forged websites: Hackers create forged websites appearing to me genuine to trick the users into perform actions using the counterfeit website/software.

3. Waterholing: In this method, the genuine website of an organization is manipulated to create loopholes which help users in obtaining confidential data from the target.

Hackers are able to identify these pathways due to flaws in the organization's systems, some of which are stated below:

1. Outdated servers: Organizations tend to not update server technology as long as it works for them. Their servers may get outdated after a point in time since hackers constantly keep developing new software and technology to surpass the security of the servers.

2. Third-party vulnerabilities: This is especially prominent in case of the financial sector. Using third-party mobile payment applications such as Venmo or PayPal pose high risk of data breaches since loopholes within the software of these mobile applications can cause compromise in the privacy of its user's data. The clause in the Terms and Conditions of these applications usually specifically state that these third-party companies are not responsible for fraudulent transactions.

They then acquire copies of software used by the organization and modify it to fit their interest. They then change source code of software, where they redirect the links from the organization's genuine software to their modified version of it. Thus, all the information entered by the user after they click the link is redirected to them and not the organization. This is usually done after analysis of transaction history throughout the financial year and the period most fit, i.e., with high transaction traffic is identified for the purpose.

4.2.3 Covering Tracks

This is considered to be the most crucial step of a cyberattack since it is hard to perform and makes it equally hard to detect the root of a cyberattack. In this step, the hacker tries to erase all traces of the cyberattacks and his own presences as a part of it by accessing information of all devices linked as a part a single chain using a technology called 'Daisy Chaining'. This essentially involves erasing the login history into the organization's system, thus making it difficult to identify the location or the IP address of the device from which the data breach was conducted.

4.3 Effects of Data breaches in the Financial Sector

Once the invaders have access to local admin privileges, they are able to access the servers, from where they are able to identify locations within the digital system where finance related data is stored. This gives them the freedom to access the organization's entire transaction history, including but not limited to personal details like date of birth, gender identity, residential address, and other bank related details such as credit/debit card details, account number, etc., of its customers. Sensitive information like passwords and pin codes are usually encrypted. However, local admin privileges can be used to decrypt the same and further use them to extract important financial information. The hackers can make use of this information to transfer funds to themselves for personal gains. Such information of users obtained by breaching data is also sold at auctions on the dark web for tremendous financial profits. All of this consequently leads to the compromise in the privacy of the data of customers of the organization.

5.0 How Cybersecurity is Useful in Mitigating the Effects

Various cybersecurity solutions can be implemented in order to secure organizational systems and mitigate the effects caused by cyberattacks. These systems can be implemented within different groups depending on their status in the organization. Some recommendations are as follows:

1. Measures to be implemented by employees:
   Employees should be informed about the need for constant vigilance for potential transactions involving cyberattacks and how to identify the same. They should be made to implement strong passwords to systems involving data belonging to the organization. They should not be allowed to download any external software without verification from higher authorities. If possible, a lockdown system should be set up, not allowing any external software to be installed into the local system of the organizations devices or servers without authorized authentication. Employees should also be informed about the right way to dispose of outdated information irrelevant to the organization to prevent it from being acquired by hackers.

2. Measures to be implemented by end-users:
   End users of the organization should be made aware of the implications of the compromise of their personal data and the need to secure the same. They should be informed of use of external authentication software using two-factor or **multi-factor authentication** to add additional password security from a third device, thus adding another layer of security to their personal data. Multi-factor authentication is a digital authentication method by which individuals are granted access to applications and/or platforms after presenting two or more pieces of evidence to verify their identity (EDUCAUSE, 2021). Since multi-factor authentication essentially produces an **OTP** (One-Time Password), this should be setup on a device that is handy and not used by other people.

3. Measures to be implemented as a part of the security software in the organization's framework:
   An organization must adapt to the **DFIR** (Digital Forensics and Incident Response) model as a part of their software security system. This is a system that can be interpreted in two parts, viz. Digital Forensics and Incident Response. Digital Response is used to identify the evidence of a cyberattack, while Incident Response is the process of proposing immediate and instant solutions to counter the same. The Incident Response model works in the following manner (Figure F. Incident Response Process Cycle):

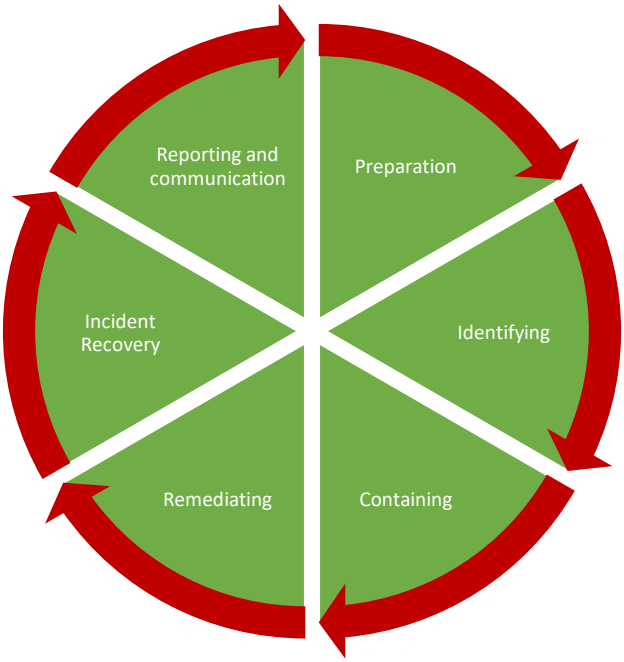


Figure F. Incident Response Process Cycle
Source: Adapted from *What is digital forensics? History, Process, Types, Challenges.* Retrieved from: https://www.guru99.com/digital-forensics.html#:~:text=Digital%20Forensics%20is%20defined%20as,phone%2C%20server%2C%20or%20network

Understanding the relevance of this model on a case-to-case basis can prove to be the best remedy for a cyberattack. This model is highly efficient since it covers all parameters to be rectified and also provides instant response to the same.

6.0 Data Breach Trends in Recent Years

In 2015 a study of data breach trends was performed by Holtfreter & Harrington, who observed the Privacy Rights Clearinghouse Data Breach Chronology (2020). Figure A. and Figure B., which were mentioned earlier in this paper, present data breach information from that data set. Holtfreter & Harrington (2015) found that "although the trends for the annual number of data breaches and their related compromised records and each of the internal and external categories have increased over the six-year period, the changes have not been consistent from year to year." The data set from this study was from the years 2005-2010. In the updated data set up to 2019, this conclusion still holds. There is most definitely an upward trend, although the year-to-year changes are irregular. Figure G. All Industries Data Breaches by Year shows data breach trends across all industries from 2005-2019.

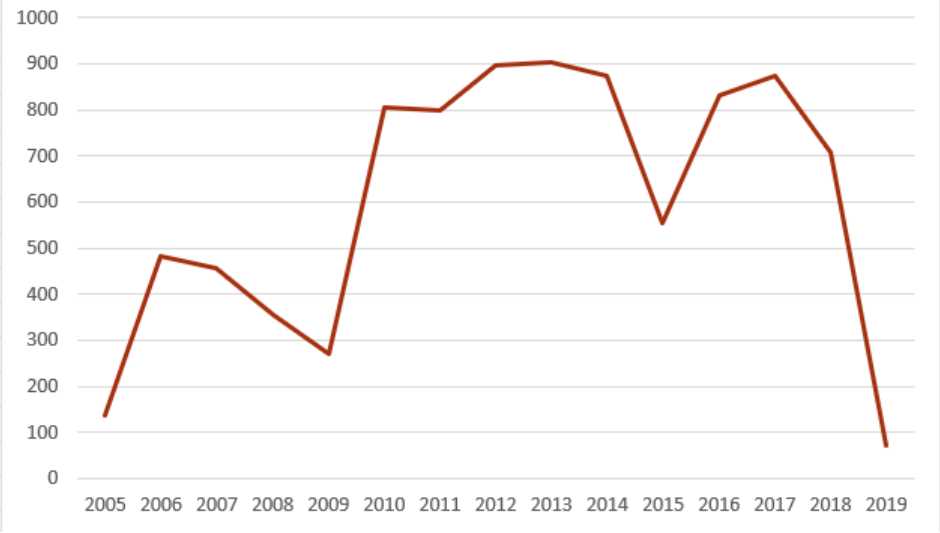


Figure G. All Industries Data Breaches by Year
Source: Adopted from Privacy Rights Clearinghouse. (2020). PRC Data Breach Chronology [Data Set]. Retrieved from https://privacyrights.org/data-breaches.

6.1 Financial and Education Data Breach Trends

From the same data set, Figure I. Education Data Breaches by Year shows all data breaches from 2005-2019 in education industries, while Figure J. Financial Sector Data Breaches by Year shows the same from the financial sector. Both show very promising downward trends, with the education data set showing more consistent year-to-year changes. With increasing cybersecurity education and improved development practices, cybersecurity vulnerabilities can be prevented (Kuhn et al., 2017). It appears that this combined with the ever-changing environment of cybersecurity vulnerabilities (Figure H. Patterns Over Time in Data Breaches) has influenced the total number of data breaches.

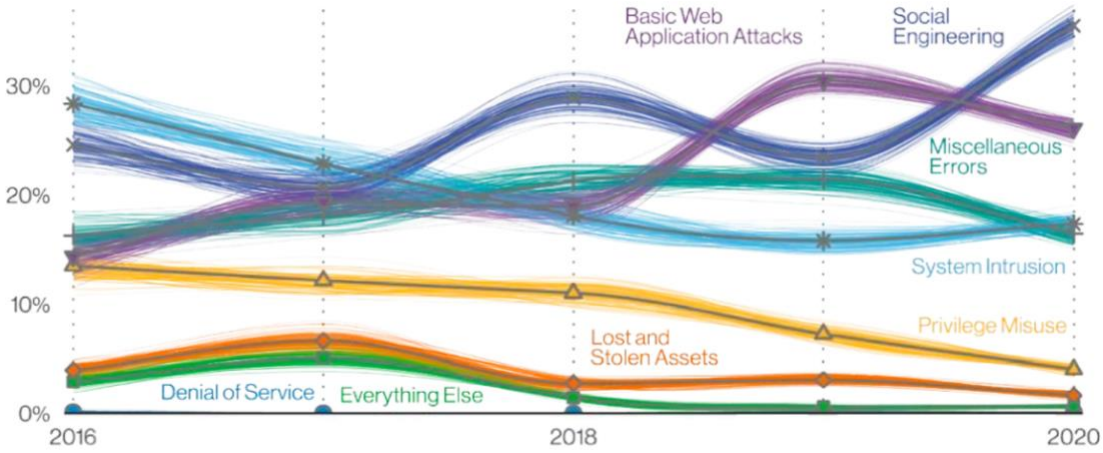


Figure H. Patterns Over Time in Breaches
Source: Adopted from Verizon. (2021). 2021 Data breach investigations report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/.

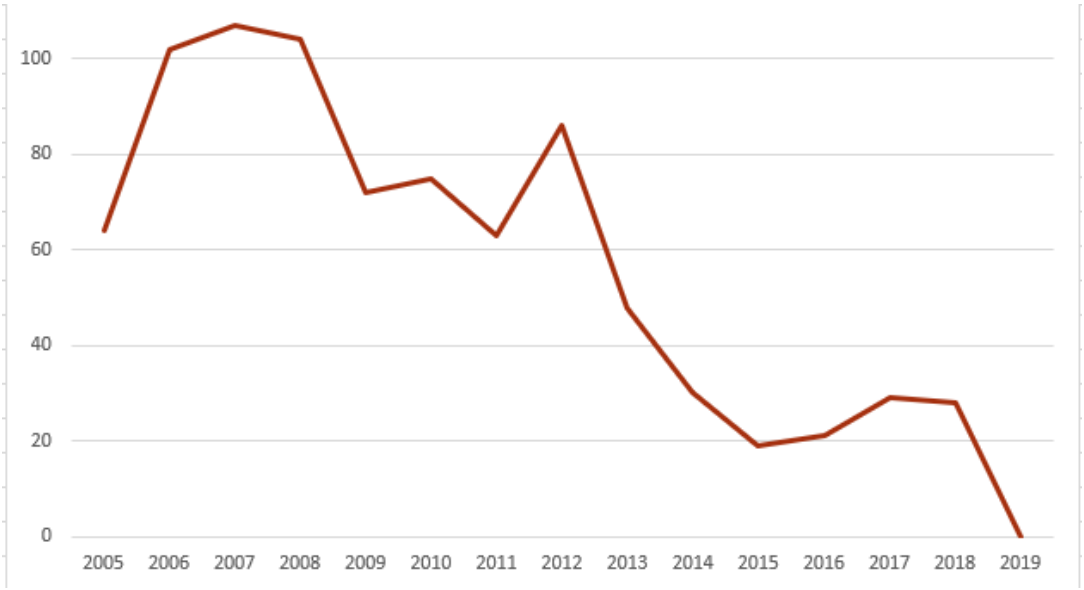


Figure I. Education Data Breaches by Year
Source: Adopted from Privacy Rights Clearinghouse. (2020). PRC Data Breach Chronology [Data Set]. Retrieved from https://privacyrights.org/data-breaches.

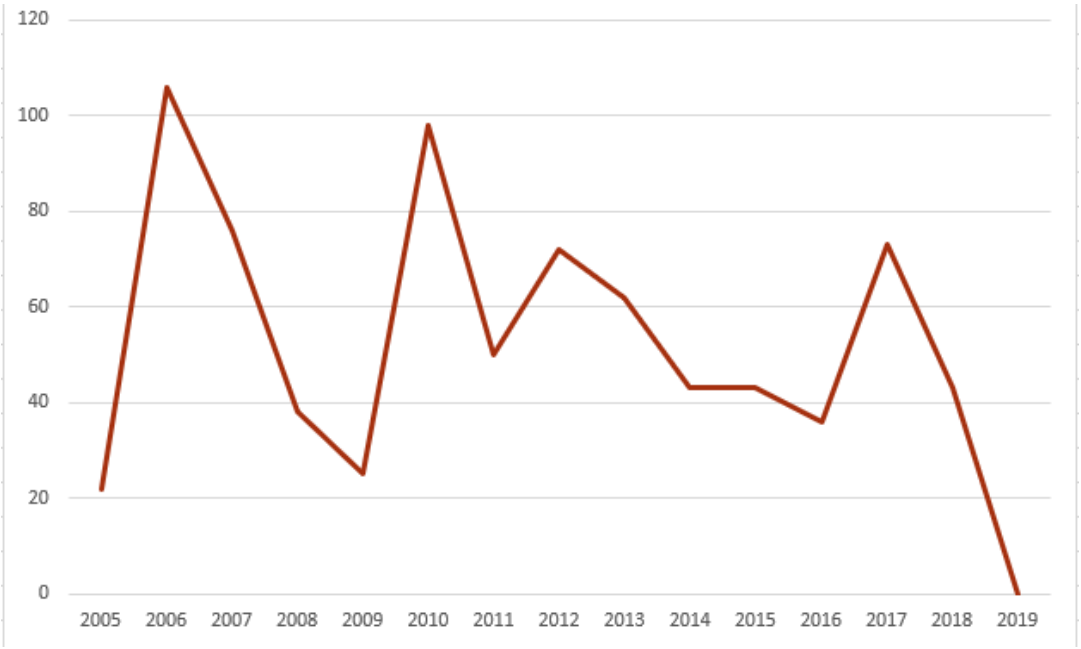


Figure J. Financial Sector Data Breaches by Year
Source: Adopted from Privacy Rights Clearinghouse. (2020). PRC Data Breach Chronology [Data Set]. Retrieved from https://privacyrights.org/data-breaches.

6.1.1 COVID-19 and Cybersecurity in Higher Education

Doug Lomsdalen is the Information Security Officer for the Information Technology Services department at Cal Poly San Luis Obispo. Mr. Lomsdalen reports to the president of Cal Poly annually regarding the current state of campus security relative to protecting university information assets.

In an email interview, Mr. Lomsdalen (personal communication, May 25, 2021) identified the biggest change that COVID-19 brought about regarding cybersecurity as the movement of the workforce towards working remotely. 80-90% of the Cal Poly workforce moved online as a result of the pandemic. This movement consists of teachers and staff members bringing home their state devices, and even using their personal computers to conduct business. According to Mr. Lomsdalen, employees working from home “distracts” them. Required online security training programs are not being completed in a timely manner. He cites a reduction in views of the security videos that are posted every month.

Additionally, ensuring that state devices remain patched has been a “constant battle”. This topic was not elaborated on, but Mr. Lomsdalen claimed that Cal Poly Information Technology Services rolled out a means to keep remote systems updated and patched as a result of the pandemic. He says that monitoring the university’s network, email services, and other key services in order to identify threats as quickly as possible are a priority for the Information Security Team.

Web services that are accessed by students and staff members of HEI are a major point of access to digital university assets (EDCAUSE, 2021). With the COVID-19’s push towards a digital workforce, these services have become even more prevalent. In an effort to increase the effectiveness of authentication for these services, Cal Poly has implemented multi-factor authentication services for member logins. Mr. Lomsdalen claims that enabling multi-factor authentication has made a

significant impact on the security of Cal Poly's campus. Since the implementation of this protocol on December 9, 2020, there has been a substantial reduction in compromised account credentials within the university (Table 2. Number of Phished/Compromised Accounts). Additionally, Mr. Lomsdalen claims that malicious threat agents are not able to do much if they eventually are able to get ahold of account credentials.

Table 2. Number of Phished/Compromised Accounts (Cal Poly, 2021)

MONTH	2019	2020	2021
JAN	1	276	28
FEB	2	64	24
MAR	7	61	40
APR	25	64	18
MAY	43	44	0
JUNE	37	17	0
JULY	22	19	0
AUG	51	18	0
SEP	142	29	0
OCT	26	25	0
NOV	57	50	0
DEC	290	40	0
TOTAL	703	707	110

NOTE: Late fall 2019, Cal Poly instituted a detection mechanism that significantly improved their alerting capability and subsequently could proactively lock accounts.

Source: Adapted from Doug Lomsdalen (personal communication, May 25, 2021).

These findings from Cal Poly can be applied to other universities as well. COVID-19 has had a similar impact across the board, not only for other HEIs, but also for other industries. The vulnerability of end-user error among employees and students is not unique to Cal Poly.

6.1.2 COVID-19 and Cybersecurity in the Financial Sector

The onset of the Covid-19 pandemic has especially posed a threat to the data privacy of the financial sector. This is due to two main reasons, the first being the world shifting all processes, including and predominantly those related to finances over to digital platforms, increasing the availability of data on the internet. Moreover, financial instability due to lack in income due to the pandemic has also caused a rise in data breaches in the financial sector. Consequently, cybersecurity is required more than ever in the financial sector and all individuals who are a part of the net banking and online transaction systems should make sure to take personal care to secure their data.

Conclusion

Although there seem to be downward trends in the amount of data breaches in the education and financial sector, the ever-changing state of cybercrime can make data breaches very difficult to predict. There is no real way of knowing if anybody's PII is safe. Social engineering attacks are on the rise, and system intrusion attacks are on the decline. However, nobody knows that the next major vulnerability will be in the coming years. Covid-19 has forced employees across almost all industries to work from home. This transition to a completely online workplace has exacerbated the problem of cybersecurity information in a way that has never been seen before. This just goes to show how unpredictable cybercrime can be. Cybercriminals will continue to find new ways to steal our data.

HEIs have unique characteristics that make them vulnerable to cybercrime, including a large number of members, values of openness in academia, as well as assets that are valuable to cybercriminals. Because of these things, social engineering attacks and hacking events are the most common data breach events in HEI. It is important to keep these things in mind, because being aware of phishing emails and scams may not only protect your individual information, but also the information of others within HEI.

A big force against cybercriminals and cybercriminals is your behavior and actions towards building a culture of cybersecurity awareness around you. It can be as simple as remembering to sign out of an account if using a publicly accessible laptop or computer. Another way to help create a positive culture of cybersecurity awareness is reminding others of the policies put in place by your HEI and making sure to follow them.

The financial sector being one of the most vulnerable to cyberattacks, will always remain under spotlight and conscious care must be taken by all individuals involved in it to secure personal sensitive data. Organizations must keep their technology to combat cyberattacks as well as employee training regarding the same regularly updated and consider that as a long-term investment for the growth of the organization.

Being aware of your information and being smart of what information you put out there is a crucial part to protect yourself from cybercriminals in any sector of society.

References

Anwar, M., Ash, I., He, W., Li, L., Xu, L., & Yuan, X. (2018). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. Oxford, England: Elsevier Ltd.

Beaudin, K. (2015). College and university data breaches: Regulating higher education cybersecurity under state and federal law. Journal of College and University Law, 41, 3, 663-666. Retrieved from https://1-next-westlaw-com.ezproxy.lib.calpoly.edu/.

Bishop, M. (2003). What is computer security? *IEEE Security & Privacy*, 1(1), 67–69.

California Attorney General (2014a). College of the Desert Data Security Breach. Retrieved from https://oag.ca.gov/ecrime/databreach/reports/sb24-45403.

California Attorney General (2014b). UC Irvine Sample Notification Letter. Retrieved from https://oag.ca.gov/ecrime/databreach/reports/sb24-45106.

California Attorney General (2020). UCOP_General_Notice CA AG. Retrieved from https://oag.ca.gov/ecrime/databreach/reports/sb24-540841.

EDUCAUSE (2021). *2021 EDUCAUSE Horizon Report: Information Security Edition*, Retrieved from https://library.educause.edu/resources/2021/2/2021-educause-horizon-report-information-security-edition.

Feri, F., Giannetti, C., & Jentzsch, N. (2016). Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior & Organization, 123*, 138-148. Amsterdam, Netherlands: Elsevier B.V.

FireEye Inc. (2015). *Why cyber attackers are targeting higher education, and what universities can do about it.* Retrieved from https://www.fireeye.com/current-threats/threat-intelligence-reports/wp-storming-the-ivory-tower.html

FireEye Inc. (2016). *Cyber threats to the education industry.* Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-education.pdf

Fisher, R., Porod, C., & Peterson, S. (2021). Motivating Employees and Organizations to Adopt a Cybersecurity-Focused Culture. *Journal of Organizational Psychology, 21(1)*, 114–121. West Palm Beach, Florida: North American Business Press

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*(2), 242–260.

James, J.G., Dominic, A. (2016). *Pass or fail? Data privacy and cybersecurity risks in higher education*. Retrieved from https://www.martindale.com/legal-news/article_mcdonald-hopkins-llc_2234700.html

Johansen, Gerard. *Digital Forensics and Incident Response*. United Kingdom, Packt Publishing, 2017.

Joy, M. S. & Shonola, S.A. (2014). Mobile learning security concerns from university students' perspectives. *2014 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL2014)*, 165-172. Thessaloniki, Greece: IEEE.

Kuhn, R., Raunak, M., & Kacker, R. (2017). It Doesn't Have to Be Like This: Cybersecurity Vulnerability Trends. IT Professional, 19(6), 66–70.

N. T. Cyriac and L. Sadath, *Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions*, 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019, pp. 380-385, doi: 10.1109/ISCON47742.2019.9036294.

Privacy Rights Clearinghouse. (2020). PRC Data Breach Chronology [Data Set]. Retrieved from https://privacyrights.org/data-breaches.

Verizon. (2021). *2021 Data breach investigations report.* Retrieved from https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

Watts, Stephen. *Digital Forensics and Incident Response (DFIR): An Introduction.* BMC Blogs, 13 Feb. 2020, www.bmc.com/blogs/dfir-digital-forensics-incident-response/#.

Glossary

Asset: Either information or business processes considered valuable by an organization.

Data breach: An event where data valuable to an organization is leaked, destroyed, manipulated, or stolen.

External data breach: A data breach involving a third party that compromises data. These data breaches can be both accidental and fraudulent.

DFIR: Digital Forensics and Incident Response.

HEI: Higher Education Institutions. This includes universities and colleges.

Internal data breach: A data breach where an employee or member of an organization compromises data.

Multi-factor authentication: A digital authentication method by which individuals are granted access to applications and/or platforms after presenting two or more pieces of evidence to verify their identity.

OTP: One-Time Password. A password that is only valid once.

PMT: Protection Motivation Theory. How people cope and make decisions during harmful or stressful events. The decisions a person makes are based on protecting oneself during the harmful or stressful events. The theory tries to explain and predict these behaviors and the motivations behind them.

Social engineering attack: An attack where a user is tricked into leaking information.

System intrusion attack: Unauthorized remote compute break-ins.

Threats: Potential instances or causes for harm to an organization.

Vulnerability: A specific weakness within an organization's attack space.