EDGUARDS

A Brief History of Higher Education Insecurity

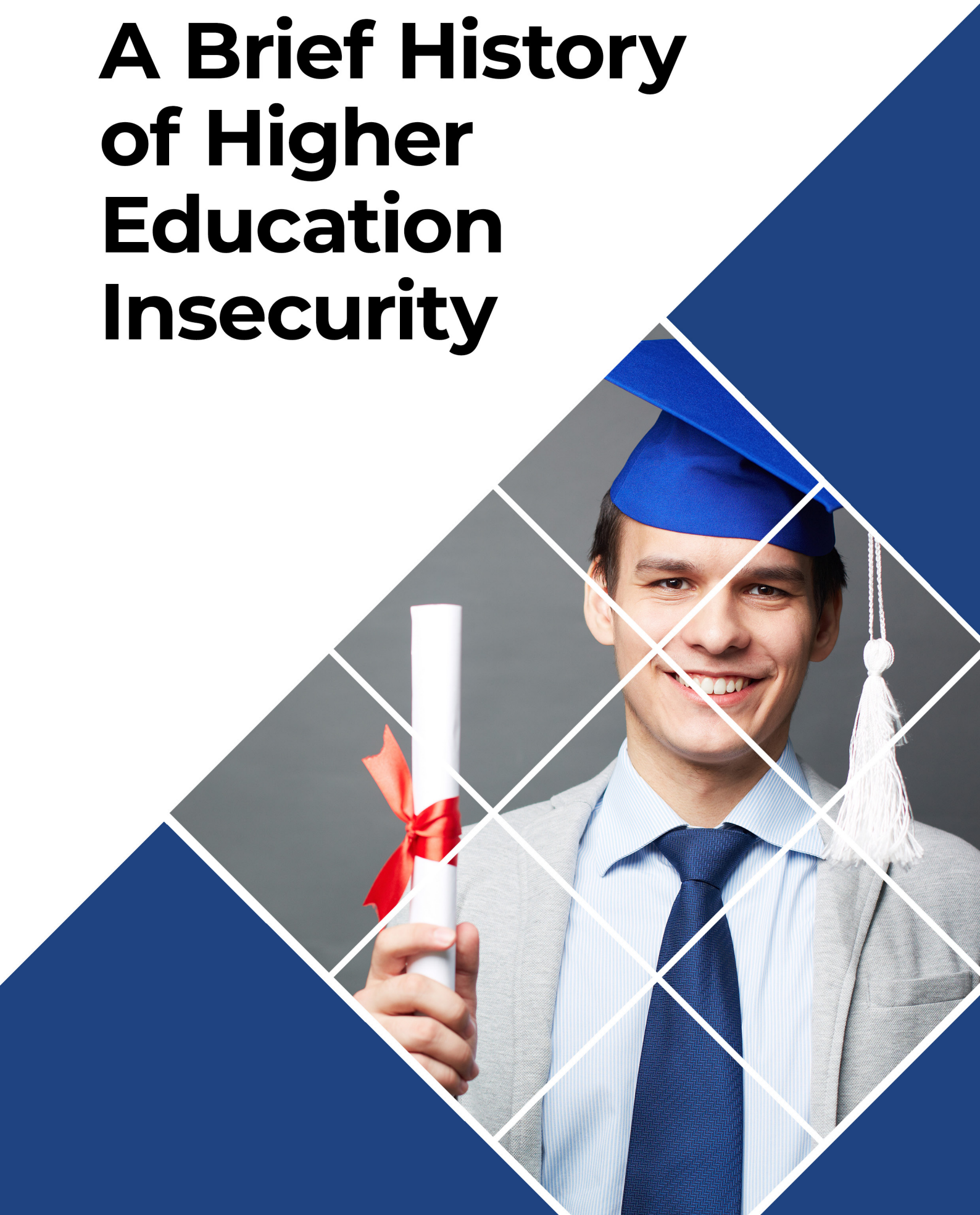

TABLE OF CONTENTS

FOREWORD

Educational institutions play a major role in the US economic, political, and intellectual well-being. Ironically, the security of the software and data systems used in such organizations on an everyday basis is far from perfect.

With this article, we offer you to take a retrospective look and see what Higher Education has irretrievably lost, what it is losing at this very moment, and what is bound to be lost unless proper protection is in place.

There is hardly an industry that a common cybercriminal would pass by. The regularity of Higher Education organizations falling victims to malefactors' actions makes them indisputable winners in the number of annual data breaches.

Among the notable cases are breaches in the University of California (2007), University of Nebraska (2012), and University of Central Florida (2016). The motivation behind the attacks may vary – it can be anything from fixing grades to stealing personal data – but the consequences are always dire. Hundreds of PeopleSoft applications worldwide are connected to the Internet, which puts them under risk. Moreover, current trend for cloud-based solutions makes sensitive data even more exposed.

HISTORY OF CYBER ATTACKS

First attacks

In the beginning, there was espionage. In 2002, malefactors from Princeton University hacked into Yale's system to pilfer information on admission decisions stored in its systems.

A year later, in 2003, a couple of incidents were said to target personal information of students and staff members. What might seem one-off incidents 15 years ago, would become a cybercriminal trend for years to come.

New law introduced

2004 proved to be a turning point in the history of cybersecurity. Back then, California passed and enacted the first 'Data Breach Notification' law. Since the day, breached organizations in California has been obliged to notify California residents whose data is stolen. That year, Californian universities reported three breaches with a total of 2,000,000 stolen records.

2,000,000
stolen records

Personal data at risk

In June 2005, a security incident took place in the University of Hawaii. A former accessed the records and stole personal data of about students, staff members, and library patrons. The total number of victims amounted to 150,000. The malefactor intended to use the data to get fraudulent loans.

The total number of victims
150,000

A similar incident happened at the University of Utah, where around 100,000 names and SSNs of former employees were stolen from archival databases of the university library.

The year 2006 brought more significant losses. About 800,000 records were stolen from the University of California at Los Angeles (UCLA) database. The leaked personal data of students, faculty, staff, parents, and applicants included names, SSNs, birth dates, home addresses, and contact information. Among the victims, there were 3,200 current or former staff or faculty members of the UC Merced and UC Oakland head departments at that time.

PeopleSoft Campus Solutions under attack

In Education, as well as in other industries, various business applications serve to facilitate the supervision of business processes. For instance, ERP systems are common in Manufacturing, while Student Information Systems are used exclusively in Education. Since these applications store and process the most critical data, cybercriminals tend to target them.

In 2007, an attack on the PeopleSoft system got wide coverage in the media. Christopher Jacquette, together with Lawrence Secrease and Marcus Barrington, used keylogging software on the computers of Florida A&M University to get the passwords and logged in to the university's PeopleSoft system to modify their grades. It did not take long for the university employees to learn about the incident, as the audit revealed both the malware and identified altered grades. This could have been the end of the story, but the trio had carried on with their attacks. That time, Jaquette received $1200 from two students who wanted to have their residency status changed to 'in-state'. The staff quickly disclosed the incident, and Jacquette was finally sentenced to 22 months in prison and three years of supervised release. Overall, about 650 grades of 90 students were modified.

An attack on a university does not always imply manipulating with students' or staff members' data. In the attack on the University of North Carolina, the hacker accessed the personal data of about 236,000 women, including about 163,000 SNNs. The records were part of the Carolina Mammography Registry, a research project that compiled and analyzed mammography data. The incident was brought to the light only two years later, in 2009. The researcher was accused of negligence, but the attorney claimed there was no evidence of violating or ignoring the rules of using the data.

Identity theft on the rise

With years, the number of attacks targeting personal data had been rising exponentially before the overall number of stolen records reached its peak of 700,000.

In 2008, a malefactor had compromised the system of Antioch University three times and gained access to about 70,000 records. The stolen data contained names, SSNs, academic records and payroll documents for current and former students, applicants and employees. Approximately the same number of personal records was leaked in a breach at the Oklahoma State University.

In 2009, Eastern Washington University informed its 130,000 current and former students that their names, SSNs, and birth dates were presumably compromised in a breach. The records dated back to 1987, so the notification process took about two weeks.

Ohio State University officials disclosed a data leak in October 2010. Unauthorized individuals got hold of 760,000 records, which included names, Social Security Numbers, dates of birth, and addresses of current and former students, faculty, staff, and university contractors. Later on, it was specified that 517,729 former students and 65,663 current students' records were compromised. It took about a month for the university to disclose the breach.

Apart from personal and financial data, there were other targets. In May 2011, the University of Wisconsin experienced a virus attack. The malware was installed on one of the university's servers. As a result, critical data of about 75,000 people including students, faculty, and staff was exposed. Despite the leak, it was presumed that the original intention behind the attack was to access the projects run by the university.

PeopleSoft is back in the spotlight

In 2012, a student at the University of Nebraska accessed the database by compromising the university's PeopleSoft system. As a result, Social Security Numbers and other sensitive data of about 654,000 students and employees was stolen, including bank account details of some 21,000 people. The database also stored information about alumni dating back to 1985.

The data from Chadron State, Peru State, and Wayne State colleges was also exposed, because the Nebraska College System had been using NeSIS, a shared student information system, since 2009. The hacker turned out to be a former UNL student. He pleaded guilty to one count of intentionally damaging a protected computer. The damage was estimated at $5,000.

Another incident took place a year later and became the third major attack on PeopleSoft. Salem State University, MT notified 25,000 students and employees about the probable compromise of their Social Security Numbers.

Data breach of 2013

Compared to other industries, attacks in Education rarely put large amounts of personal data at risk. However, in April 2013, 2.4 million personal records of current and former students and employees of the Maricopa County Community College District have been compromised. Soon after the breach, the FBI has notified the district about the stolen data, which was found on a website offering stolen records for sale.

Students have a full load, faculty work 60 hours a week, and the rest of the staff members are working on teaching, learning and research. With these busy schedules, cybersecurity awareness often takes a backseat to teaching and learning, said Bob Turner, CISO at University of Wisconsin-Madison. In this expensive arms race, it's difficult for universities to catch up with the tools that the cybersecurity industry creates given the limited resources they have…"

Bob Turner,
*CISO at University of Wisconsin-*Madison

The smarter attackers the more sophisticated attacks

2014 saw more espionage attacks against universities. Hundreds of thousands of records were exposed as a result of breaches, and attacks methods became more sophisticated and aggressive.

While their networks must be open to students, faculty, and parents, higher education institutions must also protect their business assets from the same threats that affect the commercial and government sectors.

SANS Analyst Survey
"Higher Education: Open and Secure?"

At the beginning of 2014, the University of Maryland suffered a data breach that exposed records of 309,079 people dating back to 1998.

The president of the university community, Wallace D. Loh, noted that the main question was how the attacker managed to bypass the sophisticated, multi-layered security defenses. The university authorities commented that the attackers must have had a good comprehension of the system's structure, level of encryption and database protection. Brian Voss, Vice President and Chief Information Officer at the University of Maryland, said that the incident did not resemble typical attacks where someone would leave the door open giving hackers an opportunity to get the access to the system. According to Voss, hackers picked through several locks to get to data.

The case of the University of California, Berkeley shows that detecting a vulnerability may not be enough as it can be already too late. As soon as a loophole in Berkeley Financial System was detected in November 2015, the university started to implement a security fix. Still, since the process took about two weeks, hackers had enough time to discover the vulnerability and leverage it. University officials have informed some 80,000 people about the incident. The attack could have caused huge losses, as the BFS contained the data of half of the current students and 65 percent of employees.

Sometimes, malefactors disclose an attack themselves. Metropolitan State University learned about a breach on its servers from a blog post whose author bragged about hacking Metro State's website among 75 others. The hacker seemed to be an Australian teenager. The university authorities decided to move the website to another server to prevent future attacks.

During this period, we saw a sharp increase in the number of attacks. According to the statistics provided by Verizon's annual Data Breach Investigations Report, the frequency of security breaches affecting universities have multiplied by almost ten times.

DDoS and sabotage

In 2017, the total number of incidents in Education has grown up to 393 (in contrast to only 5 in 2012). At this point, apart from the usual personal data theft, DoS attacks began to gain popularity among hackers.

One of the most unusual sabotage attacks was performed on the American university's network. As a result, some 5,000 internet-connected objects, including vending machines and light bulbs, were making DNS lookups related to seafood every 15 minutes. The attack caused internet outage almost all over the campus. The malefactor used IoT malware designed to brute force default and weak passwords of devices connected to the Internet.

Another sabotage incident is associated with Butler Community College that claimed to have suffered from a DDoS attack, resulting in temporary service interruption.

Espionage is the new trend

Although 2018 is not over yet, we can already list some noteworthy incidents.

In March, nine Iranian hackers were indicted for a massive attack on over 300 universities worldwide. The attack has affected 144 US universities and 176 universities in other 21 countries. More than 100,000 faculty members' email accounts were targeted, and about 8,000 of them were compromised.

According to the investigation, 31 terabytes of "valuable intellectual property and data" were exposed. The US Department of Justice claimed the incident should be attributed to a Tehran-based hacker clearinghouse – the Mabna Institute, which was formed in 2013 and had ties to the Islamic Revolutionary Guard Corps. This case has been characterized as one of the largest state-sponsored hacking campaigns ever.

FINAL THOUGHTS

From ransomware attacks and breaches compromising the personal information of students, faculty, and staff to denial-of-service attacks that render learning-management and other systems unavailable during important times, cybersecurity threats pose an increasingly common business risk to colleges and universities.

Deloitte Insights

We hope this brief overview gave you an understating of the cybersecurity risks faced by educational institutions. Undoubtedly, hackers will come up with new attack techniques and find other soft spots. While we cannot glimpse the future, we can make some practical conclusions about the security landscape of Education:

1. Compared to other industries, the losses of data are lower in Education, and the number of stolen records rarely reaches one million.

2. While this number is relatively low, it is mostly presented by personal data, such as Social Security Numbers and bank account details. This makes attacks and their consequences more dangerous. Stolen personal data can be further used for fraud.

3. Universities often store massive archives of data that include records of both current and former students and employees, so the possible number of victims grows.

4. The number of attacks on universities is growing much faster than in other industries. This can be explained by the relatively low levels of security and awareness. It's easier to steal data from a university than from a bank or a retailer.

5. Business applications, such as HR, Financial and Campus Solutions by PeopleSoft or other vendors, are the main target, as they store the most critical data and are vulnerable to both hackers and malicious insiders.

ABOUT US

EdGuards is a pioneer company making a breakthrough in the cyber security of Education industry with services and solutions that keep high-risk PeopleSoft applications safe from threats and data breaches. EdGuards supports and develops the EG News project intended to keep professionals updated on the latest news about Education Cybersecurity and Technology.

Serving education, our data-protection solutions are designed to address industry-specific challenges, minimize security risks organizations face today, and bring security to every department at educational institutions that use PeopleSoft applications including Human Capital Management, Financial Management, Campus Solutions, etc.

Our mission is to solve intricate security issues and most demanding challenges to guard K-12 organizations and Universities against cyber attacks. Educational organizations from all over the world trust our team and services to support them every step of the way.

CONTACT US

edguards.com

@edguardsnews

info@edguards.com

One Liberty Plaza, 165 Broadway, Suite 2301,
New York, NY 10006, US

(646) 759-3647