This article is an extract from *Performance*, Volume 8, Issue 3, August 2016. The full journal is available at **ey.com/performance**

Cybersecurity in higher education: the changing threat landscape

The particular nature of higher education institutions means they are far more prone to cyber attacks. Elements such as open networks, large volumes of data and freedom of public access expose them to a variety of cyber threats and risks. These are challenges that will only grow as cyberspace continues to evolve. In order to secure these institutions, it is important for their decision-makers to understand the threats and associated motives and, by doing so, be better placed to implement proper controls that safeguard the institution's most valuable information.

This article is an extract from *Performance*, Volume 8, Issue 3, August 2016. The full journal is available at **ey.com/performance**

Authors

Abhay Raman
Partner, Cyber Risk Services Leader, EY, Canada

Fahad Kabir
Senior Manager, Cyber Risk Services, EY, Canada

Seyed Hejazi
Manager, Cyber Risk Services, EY, Canada

Krishna Aggarwal
Senior Consultant, Cyber Risk Services, EY, Canada

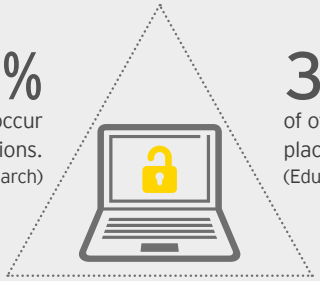
This article is an extract from *Performance*, Volume 8, Issue 3, August 2016. The full journal is available at **ey.com/performance**

While cyber threats and risks are unique to each industry, higher education is currently one of the top five sectors facing high numbers of cyber attacks. For example, recent research has identified that, every hour, one-third of universities in the UK are hit by a cyber attack.[1]

The environment in which higher education institutions operate, and the data that they store, is what makes them prime targets for a cyber attack. The campuses of higher education institutions are, often, like mini cities, due in part to the many students living on campus, but also because of local visitors and those providing services to support the various education programs on offer. A variety of data is generated and collected as a result of the support made available to the members of these institutional communities (i.e., students, faculty, staff and visitors), such as:

- Financial data relating to tuition fees and student loans, etc.
- Personally identifiable information (PII)
- Health and medical information
- Enterprise data
- Higher education operational data (e.g., grade management system and research data)

63%
of reported breaches occur in doctoral institutions. (Educause Just in Time research)



35%
of of all security breaches take place in higher education. (Educause Just in Time research)

46%
of higher education networks with breaches had verified advance persistent threat (APT) activity taking place in their environment. (FireEye)

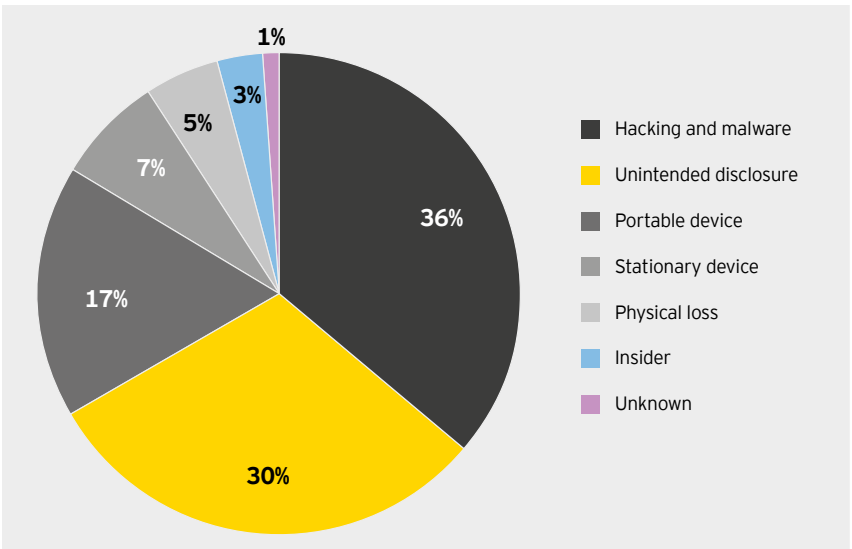
> The environment in which higher education institutions operate, and the data that they store, is what makes them prime targets for a cyber attack.

1. D. Correa, "Third of UK universities victimised by cyber-attacks," *SC Magazine*, http://www.scmagazineuk.com/third-of-uk-universities-victimised-by-cyber-attacks/article/483740/, accessed June 2016.

This article is an extract from *Performance*, Volume 8, Issue 3, August 2016. The full journal is available at **ey.com/performance**

In recent years, the number of cyber attacks on higher education institutions has seen a significant rise.

Figure 1. Types of data breaches impacting higher education institutions



This data is often stored in a variety of systems strewn across multiple departments within the institution. As a result of ever-increasing educational needs and competition in the sector, the volume and types of data collected continue to grow. And this growth carries even more risk to higher education institutions, as they become targets for identity theft or the stealing of financial information or IP. In recent years, the number of cyber attacks on higher education institutions has seen a significant rise.

This article is an extract from *Performance*, Volume 8, Issue 3, August 2016. The full journal is available at **ey.com/performance**

Pennsylvania State University, US, May 2015[2]

- The College of Engineering was targeted by two sophisticated cyber attacks that compromised servers containing records relating to 18,000 people. The attacks had been undetected on the college's network for some time.
- At least one of the two attacks was carried out by threat actors in overseas territories.
- The attack resulted in the network being unavailable for three days.

University of Maryland, US, March 2014[3]

- A cyber attack targeted the university's network, compromising 287, 580 records of students, faculty, staff and affiliated personnel.
- The database breach affected everyone who had been issued a university ID between 1998 and February 2014.

Multiple Japanese universities, July 2015[4]

- The networks of six Japanese universities came under simultaneous cyber attacks.
- On the same day, one of Japan's banks was also hit by DDoS attacks.
- One university said 360 email addresses may have leaked, while another may have lost ID numbers relating to its website admin.

University of Delaware, US, July 2013[5]

- A cyber attack on a computer system exposed the identities of more than 72,000 people.
- Hackers exploited a vulnerability in web-based software used by the university and stole names, addresses, social security numbers and university IDs of current and past employees.

King Saud University, Saudi Arabia, January 2012[6]

- The official website of King Saud University (KSU) was hacked by an unknown hacker.
- A database of 812 users was hacked, and the contents were dumped on a file-sharing site.
- The data included mail addresses, mobile phone numbers and passwords.

Concordia University, Canada, March 2016[7]

- Keyloggers, hardware devices that can capture personal data by tracking keystrokes, was found on some workstations in two of the university's libraries.
- The breach potentially impacted anyone who had used the affected computers in the past year.

2. "College of Engineering network disabled in response to sophisticated cyberattack," PennState website, http://news.psu.edu/story/357656/2015/05/15/administration/college-engineering-network-disabled-response-sophisticated, accessed June 2016. D. K. Kumar, "Cyberattack on Penn State college said to have come from China," Reuters, 2015, http://www.reuters.com/article/us-pennstate-dataprotection-idUSKBN0O01UB20150515, accessed June 2016.
3. "UMD Data Breach," University of Maryland website, http://www.umd.edu/datasecurity/, accessed June 2016.
4. "Alert raised after six universities, banks come under cyberattack," *The Japan Times*, July 2015, http://www.japantimes.co.jp/news/2015/07/14/national/alert-raised-six-universities-come-cyberattack/#.VyoJjYQrLIU, accessed June 2016.
5. "What happened in the July 2013 cyberattack at UD?" University of Delaware website, https://www.udel.edu/it/response/what.html, accessed June 2016.
6. M. Kumar, "Saudi Arabia's King Saud University Database Hacked," *The Hacker News*, January 2012, http://thehackernews.com/2012/01/saudi-arabias-king-saud-university.html, accessed June 2016.
7. K. Seidman, "Concordia warns university community about possible computer security breach," *Montreal Gazette*, March 2016, http://montrealgazette.com/news/local-news/concordia-warns-university-community-about-possible-computer-security-breach, accessed June 2016.

This article is an extract from *Performance*, Volume 8, Issue 3, August 2016. The full journal is available at **ey.com/performance**

Institutions that store research data are more likely to be targeted by organized crime syndicates or state-sponsored attackers, whereas any personal data that is hosted might be targeted by cyber stalkers.

Protecting the security of information and IT assets has always been challenging, mainly due to the unique environment and industry in which these organizations operate. Detailed here are some of the challenges that affect the ability of higher education institutions to plan and defend against cyber attacks:

- **Decentralized IT and information security practices**, which are the result of various faculties running their own IT and security departments, cause the enforcement of streamlined security practices to become very difficult.
- **Freedom of information** is woven into both the higher education sector and academic culture. One of the consequences of this is the prevalence of open networks, which may not be properly monitored for unauthorized access, unsafe internet surfing habits and malware infections.
- **Insufficient resources**, specifically information security funding challenges, are typical in many higher education organizations and prevent them from implementing the necessary controls to battle rising cyber risks.
- Campuses are the ultimate "bring-your-own-device" (BYOD) environments, and there is a **plethora of unrestrained devices**. This results in the campus IT staff having limited ability to control what machines are connected to the campus network and manage their security controls. The effect is a dramatic increase in the attack surface for the entire institution.
- Various faculties usually have computing devices used for projects or to store scientific data. In many cases, these devices may be procured by each faculty independently without following formal security architecture guidelines. **Unstructured data**, generated and processed by these computing machines, is very hard to locate, classify and safeguard.
- **Insufficient physical security** results in institutions being unable to determine the original attack vector for security incidents that have a physical element.
- **The lack of threat intelligence** collection and sharing between universities and colleges means that these institutions remain unaware of the emerging threats.

Why is the higher education industry targeted?

The motivation behind cyber attacks varies depending on the institution's size and reputation. Large research-based universities are more likely to be targeted by organized criminals or foreign governments who want to gain access to valuable research data, while small to medium-sized higher education institutions are more likely to be the targets of organized criminals or students.

During the last few years, various threat actors have shown more interest in attacking the higher education sector, motivated by a variety of reasons:

- **Hacktivists** want to provoke media exposure from the security breach and negative attention for the institution.
- **Cyber stalkers** want to cause reputational damage.
- There could be an **insider threat** that aims to manipulate the grade system or assist in an organized cyber attack.
- The threat could be **financially motivated.** for example, using ransomware to restrict access to critical data followed by a demand for a pay off.
- The threat could come from a **foreign government** that wants to gain access to leading institutions' research data (i.e., nuclear research).
- The threat could eminate from **corporate espionage.** These attacks are initiated illegally by corporations with the aim of gaining access to confidential research papers.

The attackers' motives are influenced by the type of data and the available gains, and can vary from institution to institution. For instance, those that store research data are more likely to be targeted by organized crime syndicates or state-sponsored attackers, whereas any personal data that is hosted might be targeted by cyber stalkers.

In some cases, attackers may use the higher education institutions as a means to attack other organizations or individuals. As higher education institutions may provide "back-door" access to their peers and partners, their vulnerabilities can be exploited by adversaries to gain unauthorized access to safeguarded material. Higher education institutions also provide infrastructure, such as high-speed networks, and massive computational capacities that can be used to launch attacks against others, such as Distributed Denial of Services (DDoS) attacks,

This article is an extract from *Performance*, Volume 8, Issue 3, August 2016. The full journal is available at **ey.com/performance**

sending spam emails or the creation of Botnets[8] for other malicious activities.

Lastly, the openness of these institutions' networks makes them easy targets to attack and exploit. It means they are more vulnerable to ransomware, drive-by downloads, phishing and other cyber attacks.

Cyber attacks against higher education institutions can have an operational, reputational or financial impact, depending on the nature of the attack. For example, the following are some of the potential consequences of a security breach:

- Identity theft can result in reputational damage, and could subject the institution to regulatory fines and attention.
- Reputational attacks can have a significant negative impact on competitive advantage.
- Attacks can also result in a loss of confidence in the institution among current staff, faculty, students and prospective students.
- Financially motivated attacks, such as ransomware, can have a significant financial and operational impact on the higher education institution.

How to secure your organization

The following recommendations outline some of the measures that can be taken to help protect and secure IT and information assets in higher education institutions:

1. Develop an overall information security program across the institution that clearly outlines security policies, standards and procedures for all security domains. Manage the program via a centralized information security authority and provide each faculty's IT staff with some degree of autonomy.
2. Create a security architecture function that would oversee the requirements of various infrastructure changes, computing device procurement and large initiatives, and provide standards, guidelines and reusable component catalogues for smaller projects across the institution.
3. Create a cybersecurity awareness program to train students and staff continuously on potential risks and methods of mitigating them.
4. Use strong authentication mechanisms for the office WiFi network, and segregate the network provided to students for their BYOD devices from the institution's internal network.
5. Establish processes to enable the board to provide sufficient attention to information security and for there to be ample funding for staffing and controls.
6. Identify the data that is most valuable to the institution, and implement targeted security detection and response capabilities that are tested on a regular basis through "tabletop" and "red team versus blue team" exercises.
7. Conduct external and internal penetration testing to identify vulnerabilities. Assign owners to the resulting remediation activities and track for completion.
8. Apply appropriate access governance control to enable access to be granted based on a "need to know" basis, with the appropriate segregation of duties. ■

8. Botnets are groups of computers that, unknown to their actual owners, are compromised and controlled by threat actors who use them to perform malicious activities.

This article is an extract from *Performance*, Volume 8, Issue 3, August 2016. The full journal is available at **ey.com/performance**

Helping higher education institutions build a better working world

EY has helped many higher education institutions identify and manage cybersecurity risks through providing strategic recommendations, performing investigations into cybersecurity incidents and recommending tactical initiatives. Here are some examples.

Case study 1

A higher education institution in Canada experienced a security breach that compromised its staff's credentials. An internal investigation indicated that a student had used a physical data logging device to target specific individuals and log into the institution's grade management system to compromise the integrity of its academic data.

In response to the breach, the organization produced an incident briefing report and asked EY to assess it. We conducted a series of interviews, and provided a set of tactical and strategic recommendations.

Case study 2

A higher education institution was the target of a DDoS attack that had a significant effect on its firewalls. The institution's incident response team and the firewall vendor both worked to stop the attack, but with limited success.

EY was asked to investigate what happened and what could be learned to prevent a similar attack in the future. We approached our review in three ways:

1. An analysis of traffic patterns to understand more about the details and extent of the attack
2. An architecture review to compare against leading practices and understand where improvements could be made
3. A cyber threat intelligence assessment of internet "chatter," found in deep and dark web forums, to determine if the institution was being discussed in relation to the DDoS attack

We provided tactical and strategic recommendations that included creating an incident response plan, partnering with third-party DDoS mitigation service providers, and enhancing logging and monitoring capabilities to help enable earlier identification of attacks and the ability to perform in-depth investigations.