zix®

How Zix Helps Schools Navigate an Evolving Threat Landscape

WHITEPAPER

The digital world is getting bigger.

Each day, more devices come online, and more organizations progress toward a predominantly digital information architecture. As a result, people are more productive, more efficient, and generally better off. However, the proliferation of software-based systems also creates new opportunities for criminals and new risks for everyone.

As the digital world expands, the attack surface that might be exploited by bad actors expands with it. The number of effective tools and techniques available to modern hackers is also growing, and the barrier to using those technologies and methods is getting smaller. Cybercriminal organizations and malicious individuals are capitalizing on these converging trends to wreak havoc on public- and private-sector institutions around the world. Today, high-profile security breaches victimizing governments and global corporations make headlines regularly, and countless more do significant damage but go undocumented or, worse, undetected. No corner of the internet is entirely safe from the threat of cyberattack, and the networks of certain institutions and sectors are especially vulnerable.

Higher education is one of these.

As in other sectors, digital transformation in the higher education space is progressing rapidly, and cyberattacks on institutions of higher learning are becoming more frequent. Research sponsored by IBM Security revealed that in 2017, American universities reported more than 100 confirmed data disclosures, compared with just 15 reported in 2014. According to a May 2019 report from Moody's Investors Service assessing cybersecurity risks in higher education, the sector's risk level can be characterized as "medium." Researchers leading the study found that most colleges were highly vulnerable to attacks but determined that the potential financial and reputational damage that an attack might cause is generally limited.

This assessment is at once revealing and deceptive. While the failure to secure the sensitive personal information of students, faculty, or alumni might negatively affect a school's enrollment or fundraising, researchers have found that attackers targeting universities aren't always after financial data. A 2019 Data Breach Report compiled by Verizon revealed that espionage, not identity theft, is often a primary motive in these attacks, and that schools conducting federally funded research are common targets, as are university medical centers. That doesn't change the fact that all universities are sitting on a veritable goldmine of non-employee personal information and that protecting that data should be a top priority. A security breach could compromise student privacy and have a lasting negative impact on students' academic and professional futures, and the consequences for allowing such an attack seem to be getting more severe.

A 2019 Data Breach Report compiled by Verizon revealed that espionage, not identity theft, is often a primary motive in these attacks, and that schools conducting federally funded research are common targets, as are university medical centers.

The Price of Negligence

Earlier this year, Washington State University made headlines when it agreed to pay more than $4.7 million to settle a lawsuit after a stolen hard drive gave hackers access to the confidential records of nearly 1.2 million people. The number of victims involved and the seven-figure payout that includes cash reimbursements, attorneys fees, and administrative fees (but not expenses related to the credit monitoring and insurance services WSU will provide to victims for the next two years) are atypical of cyberattacks in the sector, but perhaps not for long.

Researchers from Gemalto, echoing the findings reported by IBM, found that in 2017, breaches in the higher education space more than doubled from the year prior. In fact, the 118 successful attacks on higher learning institutions comprised 13% of all data breaches that year. Only the healthcare and financial services sectors experienced more incidents.

In 2017, 118 successful attacks on higher learning institutions comprised 13% of all data breaches.

The data also shows that cybercriminals don't discriminate when it comes to picking targets. Schools with large endowments and ample resources to devote to security have proven just as susceptible to attack as smaller institutions. In late 2018, the discovery of a data breach at Yale revealed that the personal information of 119,000 alumni, faculty, and staff may have been compromised during an attack that went unnoticed for 10 years. More recently, applicants to Oberlin College, Grinnell College, and Hamilton College received emails demanding thousands of dollars in exchange for personal information that hackers claimed to have stolen after breaching the popular Slate software system. Slate's technology is used by roughly 900 institutions around the globe, though other victims haven't yet been identified.

Each of these attacks offers a costly reminder that hackers don't see victims — just vulnerabilities. Unfortunately, many of the university employees that continue to rely on outmoded technologies and security practices don't seem to be getting the message. A general lack of awareness regarding constantly evolving cyberthreats makes school staff and administrators more likely to fall for phishing attacks, click on malicious links, or otherwise unknowingly reveal sensitive personal information.

A lack of knowledge isn't the only obstacle schools face. Almost every public- and private-sector organization must contend with a growing technological skills gap, but finding competent IT personnel with the expertise to handle higher learning's unique security challenges can be particularly difficult. Every school faces unique budget and staffing limitations, and the decision-making entities that manage risk at universities aren't always aware of the threats posed by cyberattacks or the potential consequences of such an attack. However, certain systemic attributes also make higher-learning institutions especially vulnerable.

Exploiting the System

The typical educational environment is decentralized and fragmented by design, meaning sensitive data is stored in a number of disparate systems. This gives bad actors looking for an attack surface a wide range of options. Flaws in one system or technology can provide an entry point into an institution's larger network and can render the preventive measures utilized by individual departments virtually useless.

Furthermore, the decentralization of data storage is often accompanied by a decentralized administrative structure. Because higher education institutions are highly collaborative, most veer away from a strict top-down organizational command chain. The relative autonomy found at various levels of the administrative hierarchy in most schools often leads to better student outcomes. It gives department heads and faculty the ability to identify and capitalize on beneficial partnership opportunities to enhance their research and teaching. But it also means that responsibility for securing digital systems may be spread out across a number of stakeholders, making new safeguards or institution-wide security policies harder to implement.

Corporate hierarchies tend to be more centralized, which in theory makes company networks easier to defend. For instance, most businesses can exert some level of control over the number and nature of devices accessing their private networks. Many companies equip their employees with all the devices they might need to do their jobs, while others restrict employee internet activity and monitor all employee communications. On a college campus, however, implementing and enforcing these safeguards is virtually impossible.

Administrators, faculty, and students are constantly downloading sensitive data to personal devices that may or may not be secured, and often unwittingly exposing their institution to a plethora of risks. Eventually, that continuous exposure has consequences.

Hard Lessons Learned

Colleges and universities throughout the country are searching for solutions to security problems that are often evolving more rapidly than they can be addressed. While some schools, such as Montana State, have implemented relatively sophisticated digital safeguards, others are finding out the hard way that their networks aren't as secure as they need to be. Sometimes when that happens and enough people are affected, the rest of the world finds out, too.

Back in 2014, the University of Maryland became one of the first schools to suffer a high-profile breach after thieves stole hundreds of thousands of student and personnel records. The investigation into the breach was led by the U.S. Secret Service, but the damage it caused was anything but confidential. In the aftermath, the university's reputation suffered along with its finances. The school struggled to explain to current and prospective students (as well as parents, alumni, and trustees) exactly what went wrong and how the problem was being addressed. Around the same time, separate incidents at Indiana University and the North Dakota University System shed even more light on higher learning's security shortcomings.

In those days, cybersecurity insurance was relatively rare in the space, and the direct financial costs of a data breach were harder to track. Few administrators understood the severity of the cybersecurity threat, and even fewer considered the possibility of a breach when creating their annual budgets. For some schools, the monetary cost of a security incident — including expenses associated with credit-monitoring services, litigation, forensics, call centers, public relations, and rebuilding IT systems — was an unwelcome shock.

The harsh reality is that many schools are just as vulnerable today as they were five years ago — and perhaps even more so due to the evolving nature of the cyberthreat landscape — but now most are at least prepared to pay the price of a data breach. In the case of Washington State University, for instance, that $4.7 million came out of the university's cyber-liability insurance policy and insurance provided by the state of Washington, not out of the pockets of students or donors.

For better and for worse, there is now plenty of data — derived from millions of records documenting reported breaches — that researchers and school administrators can use to calculate the financial toll associated with a security incident. A study conducted by IBM and the Ponemon Institute revealed that the cost per capita of a data breach in the education sector was about $166 in 2018 and that the average total cost of a breach was roughly $8.1 million, which is slightly more than most organizations in other sectors would expect to pay. However, these costs can be avoided. Zix offers comprehensive security solutions designed specifically for higher education institutions to ensure that these expenses remain hypothetical.

The cost per capita of a data breach in the education sector was about $166 in 2018 and that the average total cost of a breach was roughly $8.1 million, which is slightly more than most organizations in other sectors would expect to pay.

A STUDY CONDUCTED BY IBM AND THE PONEMON INSTITUTE

Minimizing Human Error

Eliminating dependencies on manual intervention and human decision-making is the first critical step every institution must take in order to reduce overall vulnerability. Human error is still the primary cause of most security incidents, which is why Zix solutions enable automatic scanning and policy-based email encryption. Employees relying on these tools don't need to worry about whether they should use encryption and don't need to remember separate protocols for email exchanges involving third parties. Furthermore, they don't need to know all of the guidelines that must be followed in order to comply with the Family Educational Rights and Privacy Act (FERPA) or other regulations, because the tools are designed to ensure compliance automatically.

Zix has also developed a comprehensive set of filters, allowing users to quickly scan emails and attachments for confidential information, including data that might be designated as personally identifiable information under FERPA or any other types of information deemed sensitive under state laws or other regulations.

Encrypting emails can be a hassle for employees who don't have specific technical experience or who aren't aware of the risks associated with transmitting non-encrypted communications containing sensitive information. ZixEncrypt eliminates this hassle, automatically scanning emails and attachments, and allowing users to easily encrypt or quarantine those that contain sensitive information. Quarantined messages are reviewable a second time, ensuring that the right messages always go to the right recipients.

Administrative teams in the higher education space are common targets for ransomware, malware, and spear-phishing attacks, and these types of malicious emails land in your employees' inboxes daily. ZixProtect thoroughly analyzes every email, searching for potentially malicious IP addresses and URLs, as well as targeted phrases, campaign patterns, and known and zero-hour malware attacks. Powered by machine learning, the technology combines real-time threat analysis and automated traffic analysis to ensure that legitimate emails always get to you but that threats never do.

Modern hackers are good at disguising malicious emails — but not good enough. ZixProtect boasts a 99.5% accuracy rate when it comes to detecting threats before they reach an employee's inbox.

ZixProtect works automatically, which means you don't have to spend time or money training your staff to use the tool. A simple user experience, combined with a highly sophisticated multilayer threat filtering system, makes ZixProtect an ideal solution for security teams in higher education. Moreover, our patented Best Method of Delivery protocol ensures that any outgoing email containing sensitive information is automatically encrypted and transferred in the most secure way possible.

ZixProtect boasts a **99.5%** accuracy rate when it comes to detecting threats before they reach an employee's inbox.

The New Normal

Less than a decade ago, cybersecurity was considered a niche. In 2020 and beyond, it's an issue of national security — and an organizational imperative. Nearly every cybersecurity incident reported by an educational institution over the past year has revealed a failure to enforce fundamental security measures, suggesting systemwide vulnerabilities that schools must address if further damage is to be prevented.

In the case of the Washington State breach, not only was confidential data unencrypted, but it was also stored in a physical location lacking basic security mechanisms. Schools that invest in sophisticated technology are undoubtedly taking cybersecurity defense seriously, but they must place an equal emphasis on raising basic security awareness among students, researchers, faculty members, and other staff members who may not fully comprehend the nature of the threats they face. Otherwise, the benefits of those technology investments will never be realized.

The alternative is to brace for an inevitable catastrophe. Let's not select that choice. Contact Zix today to learn how we can help your institution graduate to a higher level of cybersecurity.

WWW.ZIXCORP.COM
@ZIXCORP
+1 866 257 4949
SALES@ZIXCORP.COM