IDC

IDC INDUSTRY SPOTLIGHT

Sponsored by: Proofpoint

Institutions of higher education have become high-value targets of cybercriminals. As the threat landscape expands and evolves, institutions need robust cyberdefenses.

Advanced Threat Protection in Higher Education

November 2021

Written by: Matthew Leger, Research Manager, Worldwide Education Digital Transformation Strategies

An Evolving Cyberthreat Landscape

Institutions of higher education (IHEs) have unique cybersecurity needs. These institutions are creators of consequential intellectual property (IP), making them high-value targets for nefarious cybercriminals. They are also partners of private sector companies, government agencies, and other industries and have access to highly sensitive information, placing a larger target on their backs.

~~During COVID-19,~~ institutions across the world shifted to remote operations as well as remote teaching and learning. The rapid adoption and proliferation of new technical capabilities during the ~~pandemic~~ broadened the threat landscape, especially for institutions conducting early research on the coronavirus. The shift to remote was particularly challenging to IHEs because IT leaders were responsible for monitoring employee and customer (i.e., student) activity on the same network.

Even as IHEs bring many students back to campus, remote learning and hybrid learning are not going away and, as a result, neither are the cyberthreats. To support continued remote operations, IHEs are moving toward digital channel usage, ecommerce, and virtual student engagement in nearly all aspects of operations and service delivery. Additionally, the move toward multicloud and hybrid cloud, a significant focus for higher education leaders today, further exposes institutions to cyberthreats and reinforces the need to protect institutional systems and data from nefarious actors.

Beyond the systems themselves, college campuses operate — in many ways — like miniature cities, with a culture of openness, collaboration, and information or idea sharing. To make matters more challenging, faculty, staff, and students often lack proper cybersecurity hygiene, training, and awareness. As a result, they often struggle to balance openness and security or protect against basic cyberthreats.

AT A GLANCE

KEY STATS

- » 44% of educational institutions were targeted by ransomware in 2020.
- » On average, educational institutions lost $2.73 million in an average ransomware incident after accounting for the ransom paid as well as the costs associated with lost productivity, system repair, and services downtime.
- » 33% of educational officials interviewed expect to be targeted by ransomware attacks in the future.

Source: The State of Ransomware in Education 2021, Sophos

Meanwhile, ransomware, phishing, email compromise, insider threats, and attacks from organized cybercrime groups are increasingly common. Higher education was the most targeted industry for ransomware attacks during the COVID-19 pandemic (tied for number 1 with retail). As IHEs advance digital transformation (DX) and move toward permanent remote and/or hybrid learning and digital operations, higher education leaders must be vigilant in monitoring and mitigating cyberthreats and prepare for new classes of advanced email threats and attack vectors. Email remains the most common channel for opportunistic and targeted cyberattacks — and a major source of data loss. IHEs must work diligently to prohibit faculty, staff, and student information, as well as research IP, from being exfiltrated. That means deploying advanced threat protection to recognize and shut down attempts to steal or move data in an unauthorized way.

Definitions

Advanced threat protection is a security solution that defends against ~~complex malware or hacking~~ attacks that target ~~sensitive data within an organization~~. Higher education institutions must protect against many types of attacks. Complaints submitted to the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) cover an array of internet crime, including identity theft, theft of intellectual property rights, computer intrusion, economic espionage, online extortion, and international money laundering. Numerous fraud schemes such as business email compromise (BEC), identity theft, and ransomware occur from phishing (i.e., the use of unsolicited email/text messages purportedly from a legitimate source requesting personal, financial, and/or log-in credentials).

The FBI IC3 defines business email compromise as "a sophisticated scam targeting both businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques resulting in an unauthorized transfer of funds." In 2020, the FBI IC3 received over 19,000 BEC/email account compromise (EAC) complaints, with adjusted losses of over $1.8 billion.

In 2020, the IC3 received 2,474 complaints identified as ransomware, with adjusted losses of over $29.1 million. Ransomware is a form of malware that targets human and technical weaknesses in organizations and individual networks to deny the availability of critical data and systems. The FBI defines ransomware as "a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cybercriminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cybercriminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public." In 2020, 44% of education institutions around the world were victims of ransomware attacks, with institutions losing $2.73 million per incident on average from the ransom paid as well as the costs associated with services downtime, system repairs, and lost opportunities and productivity.

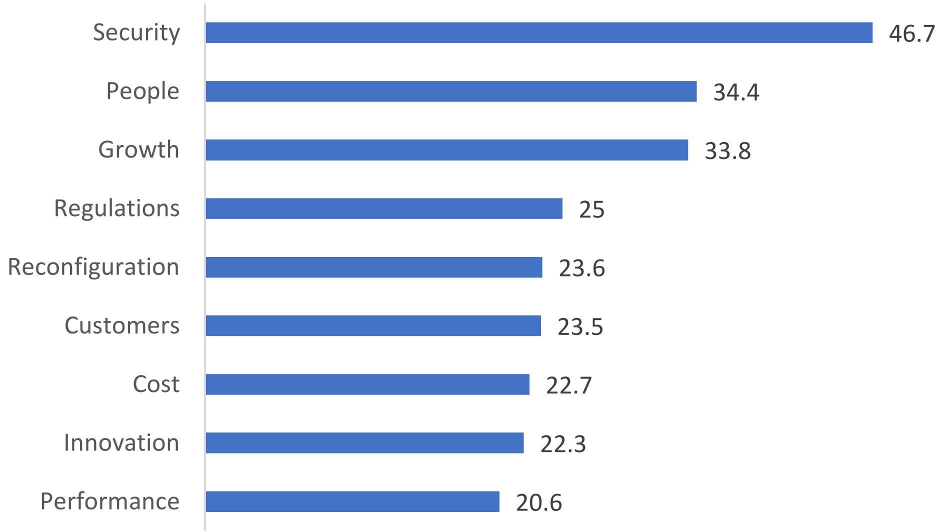
Although cybercriminals use a variety of techniques to infect victims with ransomware, according to the IC3, the most common means of infection is through spear phishing emails to end users. The cybercriminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. When the victim organization determines it is no longer able to access its data, the cyberactor demands the payment of a ransom, at which time the actor will purportedly provide an avenue to the victim to regain access to its data. Criminals may also compromise a victim's email account by using precursor malware, which enables the cybercriminal to use a victim's email account to further spread the infection.

Security Is a Top Priority for Higher Education

As IHEs look past the COVID-19 pandemic to determine their IT goals and priorities, security is the leading driver of IT investments (see Figure 1). In this context, security is defined as "strengthening detection and resilience capabilities." The second priority is "people," which refers to development and acquisition of talent. The third priority is "growth," which refers to expanding into new markets, segments, or geographies (e.g., expansion of online and hybrid learning programs).

FIGURE 1: ***Top IT Investment Priorities in Higher Education (% of Respondents)***

Q In 2020, which of the following initiatives will be significant in driving IT investments at your organization?



n = 55

Source: IDC's Industry IT and Communications Survey, July 2020

Because of the rising demand for remote and hybrid learning, IHEs will continue to leverage digital tools and capabilities not only to improve the digital learning experience but also to expand into new markets to increase enrollments. As classes continue to stay or move online, so too will student support services such as academic and career counseling as well as telehealth and mental health services. The addition of these services will increase the need to bolster cyberdefenses, particularly around email, cloud applications, and training.

Most notably, BEC should be treated as the top priority. Email is a key communication tools in higher education for faculty, staff, and students but is also the main entry point for malware, phishing, and other threats that can cause significant harm and disruption to institutional systems and their users. However, it is not enough to protect email applications and systems. It is important to ensure built-in monitoring and intelligence that yield actionable insights and enable real-time response to emerging threats.

Beyond email, the move to cloud raises additional security concerns for institutions. According to IDC's 2021 *Industry CloudPath Survey,* security is the top priority for higher education institutions as they progress through their cloud journeys. This reinforces the need to protect cloud-based systems and data from nefarious actors.

Additionally, while many higher education institutions are training the world's existing and prospective cybersecurity talent, they are not immune from the cybersecurity talent shortage themselves. Investments in people and talent apply broadly across all of IT, but people are the best defense against cyberthreats, and a big chunk of investments in people will be related to cybersecurity training and awareness.

Advanced Threat Protection Defends Against Leading and Emerging Threats

Higher education was a leading target of several sophisticated cyberthreats over the past two years following the move to online learning and operations. For example, Howard University, Sierra College, UMass Lowell, and Des Moines Area Community College were recently victims of ransomware attacks, forcing them to shut down their networks and cancel classes to address the concern. The California Community Colleges system identified more than 65,000 fake student accounts on its system, an attempt by cybercriminals to steal COVID-19 federal student relief dollars by pretending to be prospective students in need of financial aid.

Additionally, the University of Kentucky reported a data breach of one of its online learning programs, which exposed the names and contact information of more than 350,000 students who had participated in the program. While these events range in the severity of impact, they are costly, disruptive, and damaging to the reputations of the institutions. Also, with sensitive research IP, as well as sensitive student and staff information, it is critical for IHEs to prevent such occurrences to the best of their ability.

> Solutions built to prevent, filter out, and mitigate outsider contact with faculty, staff, and students through email, cloud applications, social media, and other digital channels can go a long way in preventing major disruptions.

At the root of many of these threats are touch points that expose the network and end users to nefarious actors. Solutions built to prevent, filter out, and mitigate outsider contact with faculty, staff, and students through email, cloud applications, social media, and other digital channels can go a long way in preventing major disruptions.

With these solutions in place, IHEs will be well equipped to protect themselves against cyber-risks. However, there is always a possibility that nefarious actors will bypass these defenses. To respond in these instances, IHEs need AI-driven, automated threat monitoring and intelligence capabilities to identify and flag emerging threats. Network control is needed as a last line of defense, enabling IT security personnel to intervene quickly and decisively.

Additionally, laws and regulations are constantly changing, forcing higher education institutions to adapt to changing compliance requirements. Cloud-based solutions for security compliance help institutions stay on top of regulations without forcing them to reconfigure systems on their own.

Enterprise email security, monitoring tools, and compliance management working in concert with one another are critical steps toward truly protecting the institution against ransomware and other cyberthreats. Rounding out these defenses by adding spam filtering, protection against phishing exploits, and education and training to recognize and respond to social engineering attempts provides IHEs with robust cybersecurity capabilities. The ideal goal is to protect upwards of thousands of unique end users, including faculty, staff, and students, including their email accounts and the cloud and social applications they use every day.

Key Considerations

Advanced threat protection offers tremendous benefits for IHEs, but the following are important areas for education leaders to consider when adopting the technology:

- **Balancing openness and security.** Part of what makes higher education special is the culture of openness among students to explore the world and to collaborate on research and projects. One downside of this openness is that it can inadvertently expose an institution to nefarious actors. However, it is important that institutions not lead with an iron fist when it comes to security because it may inhibit openness, creativity, and innovation that happen on campus and in the classroom or lab. Institutions should consider vendors and solutions that help balance security and openness to manage the risk/threat landscape.
- **Changing cyberinsurance policies.** In recognition that email is a leading entry point for many cybersecurity threats such as phishing and ransomware, cyberinsurance companies are implementing incentives and increasing pressure on IHEs to protect their email networks. For example, cyberinsurers are requiring customers to implement email fraud defense to simplify Domain-based Message Authentication Reporting and Conformance or risk their premiums increasing, in some cases more than doubling.
- **Ensuring proper cyberhygiene and robust training.** With many students and staff, and a sprawling physical or digital campus, it can be difficult to ensure that everyone is trained fully on proper cyberhygiene and continually informed of evolving or emerging threats. Institutions not only should emphasize ongoing training for faculty, students, and staff but also should consider weaving cybersecurity training and education into curriculums.
- **Managing security workloads.** With so many different systems, applications, and networks to monitor for threats, managing all security workloads in house can be difficult. Institutions should consider working with a vendor with proven capabilities to shoulder the cybersecurity burden, particularly around email, ransomware, cloud application, and social media monitoring and response.
- **Engendering trust through digital resiliency.** Security is about more than protecting sensitive student, faculty, staff, or institutional data. It is about engendering trust with critical stakeholders. For example, students, faculty, and staff should be able to trust that their institutions are doing all that they can to protect their information, which has implications for recruitment and retention. Security is also about building digital resiliency as institutions move toward digital services and hybrid or remote academic programs, protecting the institution against outside threats and ensuring continuity of operations.

Conclusion and Key Takeaway

Higher education institutions became leading targets for cybercriminals during the pandemic. As institutions move toward permanent online and hybrid learning, as well as digital operations, the threat landscape will continue to evolve and expand. With security as a leading priority for IHEs, protecting institutional data by deploying advanced threat protection to ensure robust cyberdefenses for email, cloud, and social applications should be at the top of the consideration set.

About the Analyst

Matthew Leger, *Research Manager, Worldwide Education Digital Transformation Strategies*

Matt Leger is Research Manager for IDC Government Insights responsible for the Worldwide Education Digital Transformation Strategies practice. Mr. Leger's research focuses on key education IT and digital transformation trends, as well as emerging solutions impacting how primary, secondary, and higher education and related services are delivered.

MESSAGE FROM THE SPONSOR

About Proofpoint

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyberattacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

More information is available at www.proofpoint.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.