A **CENTER FOR DIGITAL EDUCATION** ISSUE BRIEF | ZSCALER

Four Steps to **Manage Cyber Risk in Higher Education**

Dramatic increases in ransomware attacks and other cybersecurity breaches are creating a perfect storm for higher education institutions — and the cyber insurers they contract with to protect themselves.

Rising Risks and How to React

The education sector continues to be disproportionately targeted by ransomware and other attacks.[1] Higher education institutions also face distinct challenges, including a diverse range of stakeholders in academics, administration, research and healthcare, each of which brings with it challenges and unique regulatory requirements.

At the same time, higher ransomware demands — which have more than doubled in the last year to an average of $2.2 million per attack[2] — are having the same impact on cyber insurers as natural disasters have had on other underwriters. "As we start to see more extreme conditions, whether it happens to be weather or risk, a monetary increase will be seen in policies going forward," says Stephen Singh, head of mergers acquisitions, divestitures, private equity and cyber risk at Zscaler.

Despite the growing challenges, higher education leaders can take steps to enhance their cybersecurity posture, manage cyber risk and reduce the likelihood of successful attacks. Here are four key steps to take:

1. Apply Proper Hygiene and Controls

A first step to improving cyber posture — and becoming more insurable — is to make sure your institution is following industry best practices. These range from endpoint security and multifactor authorization (MFA) to patching existing systems, ensuring backups and data loss prevention, and training students and staff.

Multiple studies show that many organizations have either failed to adopt these practices or have incorrectly implemented them, increasing their vulnerability to attack.

"That level of efficacy is incredibly important, especially when you're trying to measure, manage, and underwrite risk," Singh says.

Document the controls and strategies put into place for both internal use and cyber insurance providers. "Don't just deploy them," Singh says. "Deploy them with a level of attribution that is meaningful to your organization and those who may be using this information to pass judgment."

2. Adopt Zero Trust

When it comes to cyber defense, most institutions have created "a hard outer shell and a very soft interior," Singh says. "Malicious actors can go anywhere they want once they get past that hardened shell."

Instead, institutions should adopt Zero Trust as a security framework. Zero Trust, which Singh describes as "a journey, not a product," is an approach that constantly verifies each user's identity as they navigate through the network.

Zero Trust ensures that users only have access to the systems and data they need, making it far less likely that entire systems or data stores will be compromised. "Once you reduce your attack surface, prevent lateral spread and stop data loss, you take an enormous amount of risk out of your system," Singh says.

IT architectures built around Zero Trust also provide data and telemetry to continuously monitor and pinpoint suspicious behavior and automatically respond based on the potential risks. Artificial intelligence and machine learning (AI/ML) are supercharging these capabilities, along with providing richer insights into where institutions should invest time and resources.

3. Use Cyber Risk Quantification

The next step requires a cultural shift in how institutions think about cyber risk. Cyber risk quantification, or CRQ, changes the conversation by assessing risk in financial terms. Institutions use risk ratings and analytics to assess the potential cost of a breach — often in the millions or tens of millions of dollars. “This level of granularity allows you to have much better insights as to what your exposure truly happens to be,” Singh says.

From there, institutions determine the extent to which investments in different cybersecurity strategies can mitigate those losses. “Each is a dial to reduce the cost to a smaller amount,” Singh says, “based on how much potential financial loss you can mitigate with the controls you implement.”

By focusing on financial issues rather than technology, CRQ also allows institutional leaders to discuss strategies with a business-focused perspective. “It changes the dialogue to something understandable by the C-suite and board of directors,” Singh says. “Rebalancing your cyber risk investment strategy becomes a much more progressive discussion with your executive team.”

In those data-informed discussions, senior leaders determine the amount of financial risk the institution is willing to accept, mitigate through investments in cybersecurity controls or transfer to cyber insurance providers.

65% of organizations still lack a cyber resilience or incident response plan to react to attacks — attacks that institutional leaders should consider inevitable.

“Financial loss is the mechanism to assure the best choice versus the first choice. The more you mitigate, the less risk you must accept, and the less you have to transfer to the underwriter,” Singh says. “That also results in more favorable cyber insurance policies, because you’re now speaking the same language.”

4. Partner with Cyber Insurance Providers

Cyber insurance providers do far more than underwrite coverage for breaches and attacks. Many now offer a wide range of services, including risk assessment and engineering, incident response and managed services. Some even offer legal and public relations services in the event of a breach.

Assume the Worst, But Plan for the Best

Above all, it’s critical to be realistic about the threats. Singh says that 65% of organizations still lack a cyber resilience or incident response plan to react to attacks — attacks that institutional leaders should consider inevitable.

“Everyone should assume you have been compromised or you will be compromised and have a plan of action,” Singh says. “The threats, risks, vulnerabilities, breaches and extortions have never changed more rapidly. Think about what the right model happens to be, so your limited dollars have the highest return on investment across your environment.”

Endnotes:
1. https://news.sophos.com/en-us/2023/07/20/the-state-of-ransomware-in-education-2023/
2. https://www.zdnet.com/article/ransomware-payments-heres-how-much-falling-victim-will-now-cost-you/

This piece was written and produced by the Center for Digital Education Content Studio, with information and input from Zscaler.

Produced by: gt CENTER FOR DIGITAL EDUCATION

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century.

www.centerdigitaled.com.

Sponsored by: zscaler™

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

www.zscaler.com

ADOBESTOCK.COM