Finding Ways to Solve the Cybersecurity Challenge

New federal mandate adds urgency to campus network security.

CYBERSECURITY HAS BEEN A KEY PRIORITY among campus IT leaders for years, but new federal requirements ramp up the importance of these efforts even further.

In a **February 2023 announcement**, the U.S. Department of Education's Federal Student Aid (FSA) office published new information security requirements for all institutions that administer federal student aid.

FSA noted that colleges and universities administering federal student aid fall under the Gramm-Leach-Bliley Act, and therefore changes to the act's Standards for Safeguarding Customer Information published by the Federal Trade Commission — which oversees compliance with the act — apply to such institutions.

Colleges and universities have until June 9, 2023, to comply with the new rules, which require institutions to:

- **Designate a qualified person who's responsible for overseeing and implementing their information security programs.**
- **Base their information security programs on a comprehensive risk assessment.**
- **Design and implement safeguards to control the risks identified in this risk assessment.**
- **Regularly test and monitor the effectiveness of these safeguards.**
- **Evaluate and adjust their information security programs in light of the results from this testing and monitoring.**

- **Implement policies and procedures to ensure that personnel can enact their information security programs effectively.**
- **Address how they'll oversee their information security providers.**

Colleges and universities that maintain information on at least 5,000 students also must create an incident response plan, and the person in charge of information security at these institutions must regularly report to the board of trustees and the executive cabinet about their information security programs.

Education Is a Growing Target

The new mandates come as education continues to account for a growing percentage of cyberattacks across all industry sectors. In fact, one industry-based assessment **noted** that the percentage of incidents targeting education jumped from 2.8 percent in 2021 to 7.3 percent in 2022.

In **separate guidance** issued to colleges and universities, FSA said it has developed a fact sheet with **advice** on how to establish an incident response plan. In addition, the agency noted that a recent report from the Cybersecurity and Infrastructure Security Agency (CISA), titled "**Partnering to Safeguard K-12 Organizations from Cybersecurity Threats**," describes how a small number of steps can reduce cybersecurity risks significantly.

Although the report is aimed at K-12 institutions, colleges and universities may find its recommendations useful as well, FSA observed. These recommendations include:

- **Develop a cyber incident response plan that leverages the NIST Cybersecurity Framework.**
- **Minimize the burden of security by migrating IT services to more secure cloud versions.**
- **Build a relationship with CISA and FBI regional cybersecurity personnel.**
- **Implement multi-factor authentication (MFA).**
- **Prioritize patch management.**
- **Perform and test data backups.**
- **Create a training and awareness campaign.**

The CISA report adds an important caveat to the above recommendations: "Change must come from the top down." It's critical for education leadership to establish and reinforce a cybersecure culture, CISA emphasized, to support cybersecurity efforts on campus. "Information technology and cybersecurity personnel cannot bear the burden alone."

CYBERSECURITY BY THE NUMBERS

64% of IT professionals in higher education say their institution was targeted by a ransomware attack in 2021.

$1.42 million is the average cost of resolving a ransomware attack in higher education. This includes not only the cost of paying the ransom, but the cost of restoring applications and data systems to their original state.

40% of colleges and universities need at least a month to recover from a ransomware attack.

Source: Sophos, "**The State of Ransomware in Education 2022**."

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes **networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions**. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.