Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

3 Key Strategies:
Safeguarding Schools from Cyber Threats

This document provides recommendations* to help institutes of higher education (IHE) address systemic cybersecurity risk. Along with each recommendation, there are key actions and related resources to help IHEs build, operate, and maintain resilient cybersecurity programs.

Recommendation 1: Invest in the Most Impactful Security Measures

In an environment of limited resources, leaders should focus security investments on the most impactful steps. IHEs should begin with a small number of prioritized investments: deploying multi-factor authentication (MFA), mitigating known exploited vulnerabilities, implementing and testing backups, regularly exercising an incident response plan, and implementing a strong cybersecurity training program. IHEs should then progress to building an enterprise cybersecurity plan aligned around the NIST Cybersecurity Framework (CSF).

1 Implement MFA

MFA is a layered approach to securing online accounts. Even if one factor (such as a password) becomes compromised, unauthorized users are generally unable to bypass the second authentication requirement. IHEs should review CISA's MFA Enhancement Guide, which provides a defined roadmap toward broad MFA adoption. Ensure that all users with elevated privileges, like system administrators, have MFA enabled for all systems.

Additional resources:

- Multifactor Authentication, CISA
- Phishing-Resistant MFA Fact Sheet, CISA

2 Prioritize Patch Management

Many attacks succeed because an institution is running vulnerable or out-of-date software. Keeping systems patched is one of the most cost-effective practices an organization can adopt to enhance its security posture. Prioritize fixing vulnerabilities listed in CISA's Known Exploited Vulnerabilities Catalog and sign up for CISA's free vulnerability scanning service to receive weekly reports.

3 Perform and Test Backups

Implementing, maintaining, and testing backups of critical data is an essential step to reducing impacts from ransomware and other damaging attacks. IHEs should identify data that is critical to its continued operations and implement backups that are separated from the operational network. Conduct recurring real-world tests to ensure that data can be readily restored from backups. Leaders should review the test restoration and address any gaps found during the exercise.

Additional resources:

- Data Backup Options, CISA

* These recommendations are based on the Cybersecurity & Infrastructure Security Agency (CISA) report Partnering to Safeguard K-12 Organizations from Cybersecurity Threats.

4 Minimize Exposure to Common Attacks

Malicious cyber actors continuously scan organizations to identify vulnerabilities and execute damaging intrusions. Every IHE should ensure that their Internet-connected assets are up-to-date and free from exploitable conditions. Enroll in CISA's free Vulnerability Scanning service and quickly address vulnerabilities identified in recurring reports. IHE's should take steps outlined by CISA's Stuff Off Search to reduce the likelihood that a malicious actor can identify assets when scanning the internet for potential victims.

5 Develop and Exercise a Cyber Incident Response Plan

Every IHE should develop an incident response plan (IRP) that spells out what the organization needs to do before, during, and after an actual or potential security incident. It should include roles and responsibilities for all major activities and an address book in case the network is down during an incident. The IRP should be approved by senior leadership and reviewed quarterly - or after a security incident.

Additional resources:

- Incident Response Plan (IRP) Basics, CISA

6 Create a Training and Awareness Campaign

Investment in training is just as important as investment in cybersecurity tools. All IHE personnel should be formally trained to understand the organization's commitment to security, what tasks they need to perform (like enabling MFA, updating their software and avoiding clicking on suspicious links), and how to report suspicious activity. Review your employee handbook to ensure it has a section on cybersecurity with information on acceptable use of technology, policies, and reporting procedures.

Additional resources:

- Federal Virtual Training Environment (FedVTE), CISA

Recommendation 2: Recognize and Actively Address Resource Constraints

Cybersecurity risk management must be elevated as a top priority for administrators and leaders at every IHE. Leaders must take creative approaches to securing necessary resources, including leveraging available grant programs, working with technology providers to enable strong security controls by default, and migrating IT services to more secure cloud versions.

1 Utilize Free or Low-Cost Services

CISA has a free Cybersecurity Services and Tools catalog, which provides a one-stop resource for IHEs of all sizes to find free public and private sector resources to reduce cybersecurity risk. Resources on this page include how to reduce the likelihood of a damaging cyber incident, detecting malicious activity quickly, responding effectively to confirmed incidents, and maximizing resilience. Evaluate your security program's needs to determine if any tools in this catalog are a fit for your needs.

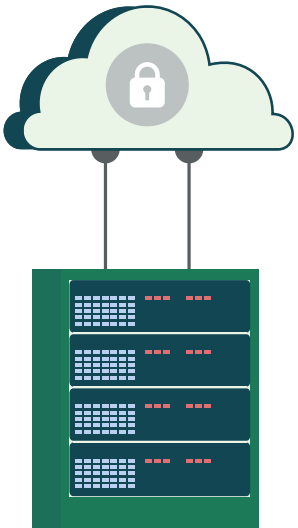
2 Ask More of Technology Providers

IHEs should expect the technology used for core educational functions, such as learning management and student administrative systems, have strong security controls enabled by default for no additional charge. During the technology procurement and renewal process, ensure that vendors do not charge more for security features like MFA and logs. Be aware of the "SSO tax", the practice of charging customers more to connect a service to a school's Single Sign On (SSO) portal. As you deploy products, review the product's "hardening guide" - a set of steps to make the product more secure.

Additional resources:

- Cyber Security Advisors at CISA Regional Offices

3 Minimize the Burden of Security



On-premises IT systems require significant time to patch, monitor, and respond to security threats. IHEs should consider migrating on-premises IT services to cloud versions for a more secure and resilient option. Prioritize migrating identity services and mail systems as they are high-priority targets for attackers. Talk to your CISA regional representative for guidance on secure cloud migration. A list of common cloud business resources are listed below:

- Azure Active Directory, Microsoft Azure
- Google Workspace
- Microsoft 365

Note: FSA does not attest to the suitability or effectiveness of these services and tools. FSA does not endorse any commercial product or service.

Recommendation 3: Focus on Collaboration and Information Sharing

Information sharing and collaboration with peers and partners is essential to building awareness and sustaining resilience. IHEs should join cybersecurity collaboration groups such as the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC community members receive critical alerts on current threats, risks, and vulnerabilities; free cyber tools, resources, and services; and 24/7 access to assistance that includes threat incident analysis, mitigation, and remediation.

IHEs should also establish a relationship with their local FBI field office and regional CISA cybersecurity advisor. This will open lines of communication on evolving threats and risks and ensure prompt provision of U.S. government assistance to prevent and, where needed, respond to cybersecurity risks.

Additional resources:

- State Information Sharing Tool, SchoolSafety.gov
- CISA Cybersecurity Advisors
- Internet Crime Complaint Center (IC3), FBI

Report a Breach

It is critical that IHEs report every breach to the U.S. government. Reporting incidents allows FSA and our partners to offer incident response assistance, help protect other potential victims, better understand our adversary to develop more effective guidance, and help law enforcement partners identify perpetrators.

Report a breach using FSA's Report a Breach intake form or by emailing FSASchoolCyberSafety@ed.gov.

Contact Us

If you have questions about the information included here, please contact FSASchoolCyberSafety@ed.gov.

Find more FSA cybersecurity resources on our website: fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity.

Additional Resources and Training

- Cyber Safety Videos, Cyber.org and CISA: This video series provides tips for staying safe online. Topics include: the Internet of Things; Social Media Safety; Ransomware; Phishing; Making Strong Passwords; Online Gaming Safety; and Video Call Safety.
- Cybersecurity Training and Exercises, CISA: This webpage lists CISA trainings available to non-federal cybersecurity professionals and the public.
- Don't Wake Up to a Ransomware Attack, National Initiative for Cybersecurity Careers and Studies (NICCS): This free online, self-paced course provides essential knowledge and reviews real-life examples of cyber attacks to help organizations prevent, mitigate, and respond to the ever-evolving threat of ransomware.
- Federal Virtual Training Environment (FedVTE) Public Courses: This training environment offers more than 800 hours of free online, on-demand cybersecurity training.
- Foundations of Cybersecurity Management, NICCS: This free online, instructor-led course teaches how to apply the principles of cybersecurity management.
- Fundamentals of Cyber Risk Management, NICCS: This free online, self-paced course focuses on key concepts, issues, and considerations for managing cyber risk.
- NICCS Education and Training Catalog: This catalog is a central location to help cybersecurity professionals of all skill levels find cybersecurity-related courses online and in person.
- picoCTF by Carnegie Mellon University: This free program combines computer security education with capture-the-flag puzzles and was created by security and privacy experts at Carnegie Mellon University.

Note: FSA does not attest to the suitability or effectiveness of these services and tools. FSA does not endorse any commercial product or service.