At-a-Glance

Managing Higher Education Cybersecurity: Think Holistically

Cyberattacks are evolving into an increasingly sophisticated for-profit business. Academic research, personal data, and disruption of operations provide attractive targets for both internet criminals and nation states. Colleges and universities must find ways to counter threats to these while maintaining a networking environment that fosters learning.

Higher education institutions have publicly announced cybersecurity incidents, such as:

- Multiple DDoS attacks that resulted in disruptions to the network. Some of these attacks occurred during key times of the year such as student class registration.
- Cyber attack originating from a foreign nation state, targeting their school of engineering
- Email systems compromised
- Breach of university health system network may have exposed sensitive information of up to 4 million patients.

To effectively protect your student information and institution's reputation, consider these three critical pillars of protection:

1) Administrative

Often overlooked, policies and training are vital. Have you:

- Created thorough written security policies?
- Established adequate cybersecurity awareness for all faculty, staff, and students?
- Regularly performed penetration testing to see if your current measures are working and to see what needs to be improved? Have you held a cybersecurity "fire drill?" Have you created a plan of action in the event you have been hacked?
- Backed up your critical data?
- Tested your recovery procedures?

The most common security threats include malware, spyware, denial of service, ransomware, data exfiltration, website defacement, and phishing. In the first quarter of 2016 criminals earned $209M* from ransomware. Can your institution afford to pay ransom to get its information back? In the case of data exfiltration, what is liability for exposing personal information or the loss of intellectual property?

* Source: money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

Table 1

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

2) Physical

Strong physical security measures are vital to ensure a safe campus.

- Are your systems truly protected where they reside? How, precisely? Have you tested them?
- Do you adequately control who has physical access to them?
- Do you keep paper records? Who has access to those?
- How would you know who was responsible if someone stole records or a computer?

3) Technical

The security industry likes to focus on technical controls because they are the most complex and potentially confusing to customers. However, technology is not a panacea, especially when it comes to security. Have you:

- Considered a holistic security solution, which can enable you to economically and smoothly explore the specific protections technical controls can provide?
- Already combined technical measures with physical and administrative controls?
- Mitigated complexity by efficiently aligning your specific security requirements to specific technology solutions?

Cisco cybersecurity solutions enable you to strategically choose to invest in the capabilities you need while remaining flexible when budgets, security policies and priorities change. For this approach to work best, each component must be able to work seamlessly with any other components. Measured against these criteria, many if not most technical solutions will not qualify.

Define a Cybersecurity Plan

The National Institute of Standards and Technology (NIST) framework provides an outline for defining an organization's cybersecurity requirements and activities. It allows one to categorize security requirements across an organization by breaking them down into functions and categories. (See Table 1) Using this frame work one can develop a more holistic view of their security needs. Using the extensible framework organizations can better define and mitigate their cybersecurity risks. For more information on the NIST framework, visit: nist.gov/cyberframework/

To properly assess your security, ask:

- Am I ready for attacks that are increasingly complex and persistent?
- How is my most sensitive information protected?
- Do you address how students and staff access the Internet and how your internal systems are protected?
- As enhanced security features are configured, how is overall performance impacted?

Next Steps for Smarter Security

- Institute identity management and policies to specify which students, visitors, staff and devices are allowed on the network – and what they are allowed to do
- Attempt to minimize the attack surface through micro segmentation.
- Implement DDoS protection and flow analysis at the perimeter to help mitigate attempts to impair network performance and services.
- Enable flow analysis throughout the network. By establishing a network flow baseline and performing flow analysis one can better detect and mitigate internal threats such as botnets, data exfiltration, and other attack that originate from the internal network.
- Consider a network visibility solution so you can be aware of suspicious traffic on your internal networks behind the Internet perimeter
- Add malware protection to combat the most complex and pervasive file-based security threats
- Reputation based security to help warn end users of malicious internet sites responsible for phishing, botnets, and other malicious activities
- Implement a robust remote access solution to ensure that sensitive data isn't captured when students and staff access your systems from home

Security Services – a Simpler Path to Safety

Do you have any security experts on staff? Would your staff know what to do in the event of an incident? Consider adding managed security services from Cisco, or our partners, if your team doesn't have the budget, time or technical expertise to address these vital issues.

Why Cisco

Cisco's cybersecurity solutions span several categorizes of the NIST framework. Our cybersecurity architecture works for you and with you. In addition to providing best of breed offerings, Cisco cybersecurity solutions were designed with integration in mind. Cisco's solutions were designed with key functions and features to allow an integrated an consistent security implementation across the various solutions. With solutions that tie seamlessly into your existing digital campus infrastructure, it accommodates individual requirements and protects against advanced threats. You can choose from:

- Perimeter Protection with next-generation firewalls, intrusion prevention, and DDoS
- Identity and Security Policy Management to control access to campus resources based on business role, device type, location, and other contextual information.
- Network segmentation based on security policy to control access and reduce attack surface
- Network Visibility for deep insight into any suspicious activity
- Malware Protection, including a collective intelligence threat database for faster awareness and accuracy
- Remote Access Controls to ensure safer access to the digital campus network
- Security Services to give your staff quick access to our network and security experts along with continuous monitoring

For more information, please visit:

cs.co/Edu-Security-ResourceKit

C45-123456-00 06/16