Information Security Roadmap Update

VERMONT
STATE COLLEGES SYSTEM

Recap Since We Last Met

- Monthly vulnerability reviews with all locations
  - Significant reduction in open vulnerabilities
- Security Council
  - Monthly to bi-monthly meetings
  - Decision-making body for security standards and procedures
- 3rd Party review process
  - Vendors with access to personal or confidential information must complete a security assessment
- Hardware/software review process
  - All new hardware/software acquisitions must be approved by IT and security team where applicable
- C2 Security assessment recommendations
  - Backup and recovery strategy
  - MFA
  - Access controls
- Policy updates, several in progress
  - Acceptable Use, Conditions of Use, Elevated Access, Equipment Hardening
- Stakeholders/Transformation - brought many items through discovery/design stage gate
- MFA
  - In flight, targeting launch in June

VERMONT STATE COLLEGES SYSTEM

Base Level Capabilities for an Effective IT Security Program

Prevention	Detection	Mitigation	Recovery
Education	Mail Filtering	3rd Party Emergency Support	Enterprise Backup and Recovery Platform*
Vulnerability Scanning	Virus and Malware Protection	*Incident and Ransomware Response Plans**	Critical System Recovery Plans*
Firewalls	*Security Information Event Management (SIEM)**	Staffing Resources or SOC Support	
Access Controls	Advanced Threat Detection	Critical Application Support (O365)	
Virus and Malware Protection			
*Multifactor Authentication**			
*Privileged Access Management**			
*Asset Management**			
Penetration Test			

Policies, Procedures, Audit and Leadership Support

Sufficient Capability In Place

Partial Capability or In Progress

No Capability

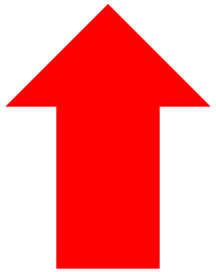
VERMONT STATE COLLEGES SYSTEM

** Cyber Insurance Requirement*

Next Steps

- Multifactor Authentication
- Security Information Event Management Platform
- Privileged Access Management Platform
- Asset Management and Discovery
- Operational Best Practices

Cyber Insurance Requirement



- Critical Applications Vendor Support
- Resources
- Vendor Partnerships

Critical Enabler

VERMONT STATE COLLEGES SYSTEM

Thank you! Questions?

VERMONT
STATE COLLEGES SYSTEM

Why is this important?

What are we Protecting?

- Organization Data
- Employee and Student Data
- Ability to Deliver Education

What are protecting it From?

- IT Interruption and Outages
- Ransomware
- Account Theft
- Data Theft and/or Destruction

What are the Costs of Data Breach

- Average cost per data breach: $4.24mm
- Cost Per Record Stolen: $180
- Average Cost per Ransomware Event: $1.8mm
- Public Relations Impact
- Regulatory Scrutiny

What Capabilities Need Attention	What Are The Risks	What Do We Need to Do
• Access Controls	• Unauthorized users with stolen credentials could remove sensitive information from our environment. • Unauthorized devices can introduce ransomware or other malware into the into the environment.	• Harden access controls to leverage multifactor authentication • Implement a platform and process to scan for unauthorized equipment in our environment
• Super and Administrative User Controls (Software and Hardware)	• These users have significant access to applications and hardware including local PCs. If their account is compromised the perpetrator will get the same access.	• Ensure only users with a need for elevated access can obtain it, only when they need it • Have the ability to monitor usage of privileged accounts • Ensure all users with elevated access are reviewed periodically
• Backup and Recovery Policies and Standards	• In the event of a major outage or security incident, inadequate backups may make restoration of data impossible	• Set minimum standards for backups and develop a roadmap for backup and recovery strategy
• Resources and Critical Applications Support	• We do not have the resources to properly investigate security incidents which can lead to a major incident • We have mission critical applications without vendor support (O365)	• Build a basic investigative security capability and acquire the tools needed to manage security incidents • Ensure as we add new capabilities, we have adequate support before implementation.

• Operational Best Practices	• Without basic governance processes we run the risk of a security incident
	  • User True Ups
	  • Access Reviews
	  • Policies
	  • Disaster Recovery
		• Continue to expand governance programs
		• Continue to update existing and develop new policies