

BUT FIRST A MESSAGE FROM OUR SPONSOR...



- This webinar is part of our monthly webinar series to stay engaged with our community and bring programming of interest to our members.
- This webinar is eligible for CPE. If you are interested in receiving CPE credit for this webinar, please e-mail me (Marty Mickey) at mmickey@nl.edu now.
- During the webinar, there will be three check in questions for you to answer. **In order to receive CPE, you must answer all three of these questions.**
- The presentation is being recorded and both the recording and a copy of the slides will be added to the CACUBO web site in the next couple of days.
- We will send out a survey afterwards to solicit thoughts and topics for future webinars.
- If you would be willing to present in a future webinar, please e-mail me at mmickey@nl.edu.

PRESENTER

Bob Eckman, CISSP, PMP, MBA

He/Him

Sr. Director Cyber Resiliency

Bob.Eckman@rsmus.com



Bob Eckman is a Sr. Director in the Security, Privacy, and Risk Consulting practice and RSM's national leader for cyber resiliency. He has over 20 years of information security and IT leadership experience. As an experienced Chief Information Security Officer, Bob specializes in critical infrastructure and higher education, healthcare, finance, and manufacturing security and resiliency. He has served on many boards, is recognized as a thought leader and security evangelist, as well as an award-winning cybersecurity adjunct professor who has been recognized by the Ohio Senate for his achievements in security.

John MacDonald

He/Him






Risk Consulting Director

John.MacDonald@rsmus.com



John MacDonald is a Director in the Risk Consulting practice at RSM. He has over 14 years of audit, risk and compliance experience. John specializes in IT strategy and governance with a focus on cybersecurity, innovation and digital transformation for the financial services industry. John serves as the National IT Risk Methodology, Automation and Enablement leader responsible for developing methodology to address changes in IT regulations. John is also the lead developer of the methodology used nationally at RSM to evaluate an organizations' compliance with GLBA, FFIEC, FedLine and CFPB IT requirements.

LEARNING OBJECTIVES

	DATA PRIVACY DRIVERS <i>Business Interruption, constituent privacy, and resiliency</i>	5
	OVERVIEW OF THE SAFEGUARDS RULE <i>Educate leaders about the requirements of the new rule</i>	7
	INFORMATION SECURITY NEW PROGRAM ELEMENTS <i>Understand the minimum requirements of an information security program</i>	6
	AND NOW A LITTLE GOOD NEWS... <i>FTC announces 6 month extension to the 12/22 mandate</i>	8
	INFORMATION SECURITY PROGRAM – SAFEGUARDS CONTROLS <i>Assigning controls to manage risks</i>	9
	INFORMATION SECURITY PROGRAM – SAFEGUARDS CONTROLS <i>7 Controls for risk mitigation</i>	11
	THE PENETRATION TEST MANDATE <i>More focus on testing and monitoring controls</i>	12
	LESSONS LEARNED <i>Some take-a-way parting thoughts</i>	13

DATA PRIVACY DRIVERS

Higher Education Security in the spotlight:

- Environments are typically very flat and open.
- Culture and higher educational data.
- Highly transitory populations, highly diverse technology needs, lack of clarity for data ownership.
- Use of Student Financial Aid (SFA) data on the rise.
- Cyber insurance mandates are evolving.

Why Universities need to focus on SFA specifically:

CYBER INSURANCE

- 61% utilize cyber insurance, 67% of those reported **increased policy premiums**.
- Loss of SFA = Business Interruption and disruption which is a **4x multiplier** on cyber claims (Net D)
- Supplementals as **“attestations”**: CIA/D2 shifting towards cyber resiliency.

H-Ed DATA CONCERNS

- Universities use of student financial aid : **“The 4 Ment’s”**
 - Recruitment
 - Enrollment
 - Fulfillment (SRM)
 - Advancement
- SFA related data is used at every stage of the student experience and managed differently at each stage.

LITIGATION

- 100,000’s active identities, GB-TB of SFA Data.
- Represents **“the golden ring”** for hackers
- **Student Safety** is every university’s primary mission. A breach of this data impacts student, faculty, and staff financial wellness and security.

Polling Question #1

Business Interruption represents a “N” multiplier on cyber claims?

- A. 2
- B. 3
- C. 4
- D. 5

OVERVIEW OF SAFEGUARDS RULE

The term “Safeguards Rule” refers to the regulations issued by the Federal financial regulators to implement the data security provisions of the Gramm Leach-Bliley Act (GLBA). “This law applies to how higher education institutions **collect, store, and use Student Financial Aid (SFA) records** (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information.”¹

The Federal Trade Commission (“FTC”) has federal rulemaking authority to issue industry-wide regulations for all entities not subject to the jurisdiction of other Federal financial regulators and has issued its Privacy Rule (16 CFR 313) and a Safeguards Rule (16 CFR 314 amended in 2021).

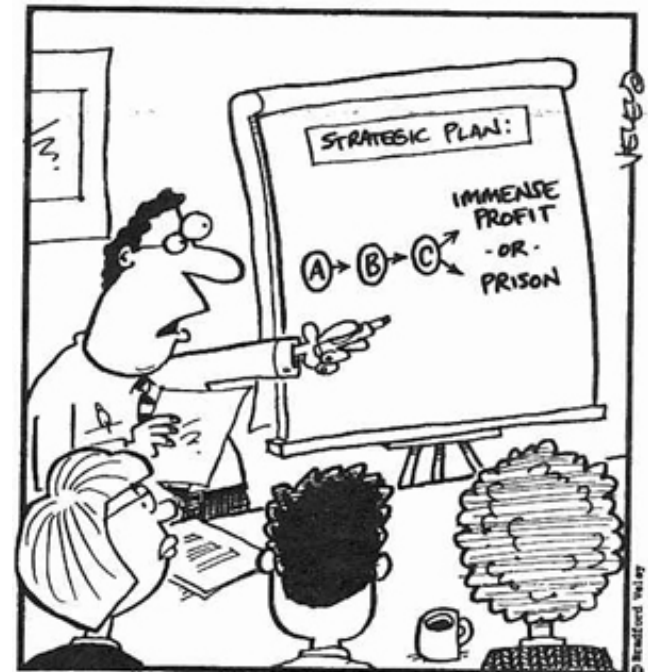
“The Secretary considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability as stated in 34 C.F.R. § 668.16(c).”

Program Participation Agreement, General Terms and Conditions Section 3.e

How might they find you?

- *Consumer complaints*
- *Internal breach requiring notifications*
- *Darkweb scanning or unauthorized release of SFA Data*

1. Educause: <https://library.educause.edu/topics/policy-and-law/gramm-leach-bliley-act-glb-act>



“Stay with me now, people, because in step C, things get a bit delicate.”

FTC EXTENSION – JUNE 9, 2023



FTC Extends Deadline by Six Months for Compliance with Some Changes to Financial Data Security Rule

Financial institutions covered by the Safeguards Rule must comply with certain provisions by June 9, 2023

provisions of the updated rule specifically affected by the six-month extension include requirements that covered financial institutions:

- designate a qualified individual to oversee their information security program,
- develop a written risk assessment,
- limit and monitor who can access sensitive customer information,
- encrypt all sensitive information,
- train security personnel,
- develop an incident response plan,
- periodically assess the security practices of service providers, and
- implement multi-factor authentication or another method with equivalent protection for any individual accessing customer information.

Key Reminders

Extension: The deadline for complying with some of the updated requirements of the Safeguards Rule is now June 9, 2023.

Rational for Change:

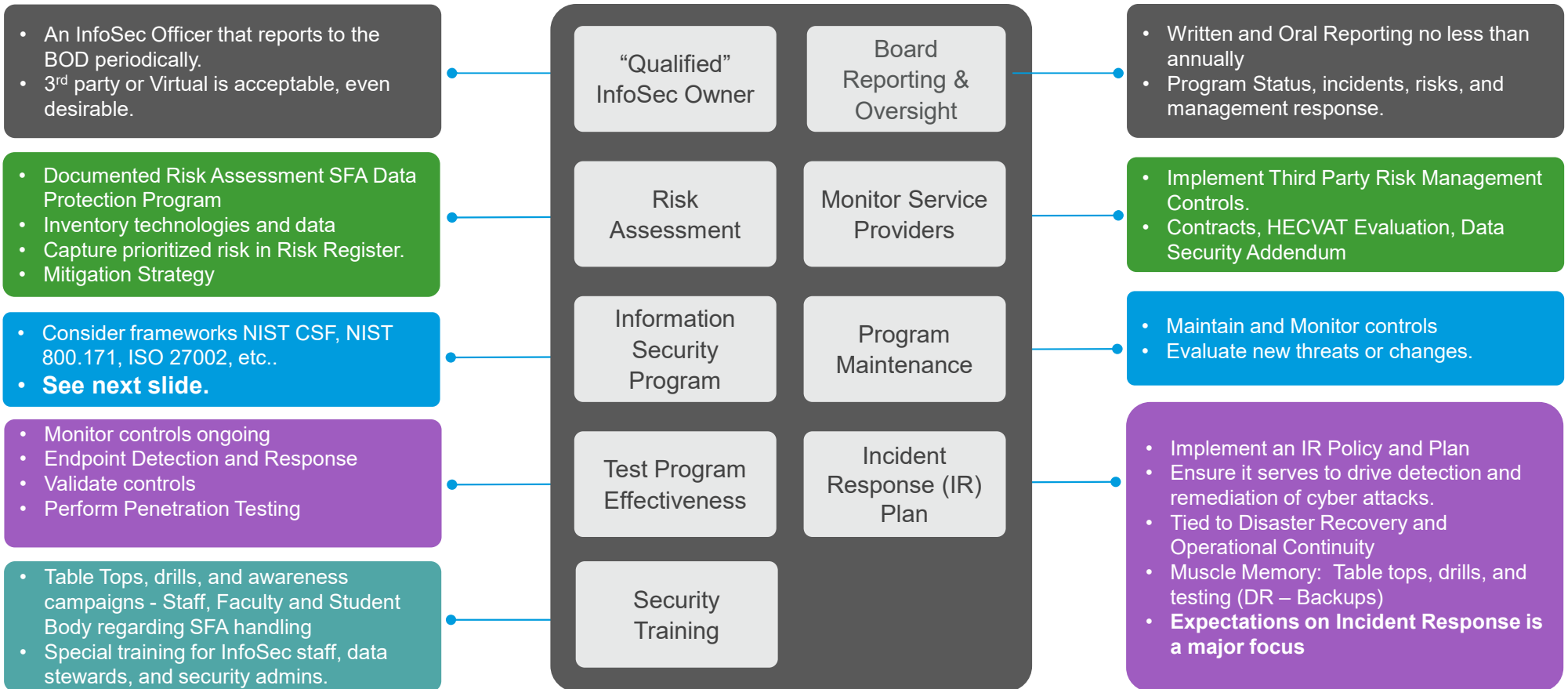
- Shortage of skilled personnel
- COVID-19 Pandemic
- Advocacy by Small Businesses

Reminders:

- Create YOUR plan / Don't wait!
- Educate your board
- Cyber breaches require notification to the FTC
- Continue to monitor student complaints (attorney general, BBB, CFPB, etc.)
- Leverage industry associations and councils to identify best practices and opportunities for economies of scale

INFORMATION SECURITY NEW PROGRAM ELEMENTS

Section 314.4 of the Safeguards Rule identifies nine (9) elements that your company's information security program must include:



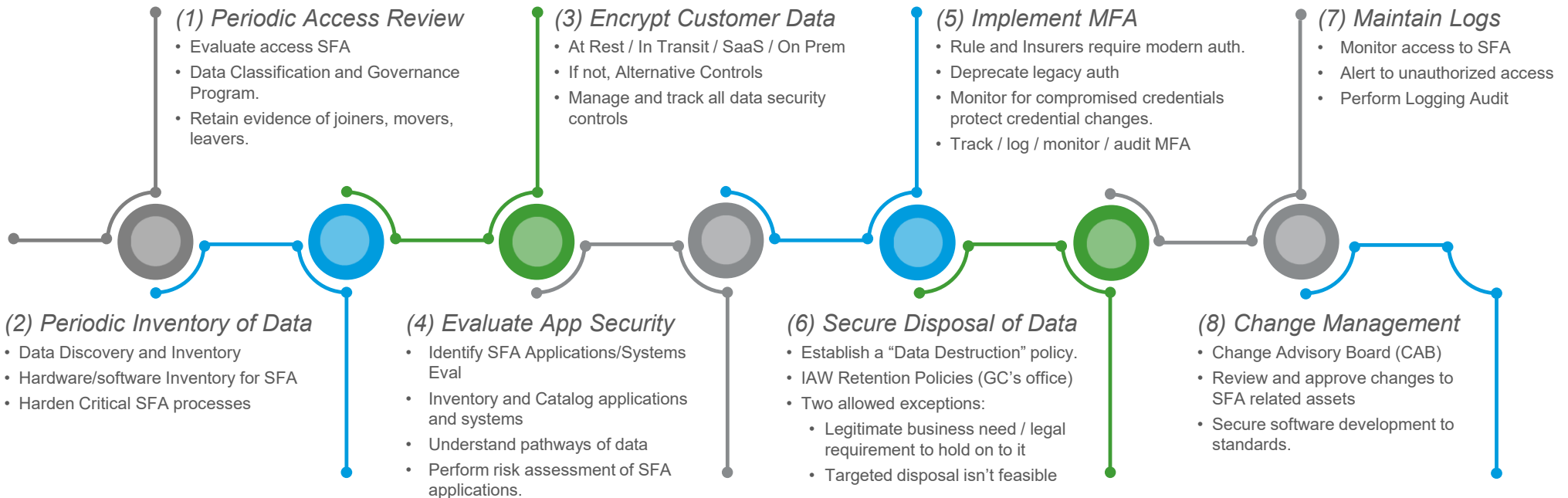
Polling Question #2

HECVAT stands for?

- A. Hospital Evaluation of Computer Venders and Technologies
- B. Higher Education Cloud Vendor Assessment Tool
- C. HITRUST Education Community Vendor Assessment Tool
- D. Higher Education Community Vendor Assessment Tool

INFORMATION SECURITY PROGRAM – SAFEGUARDS CONTROLS

(c) Design and implement safeguards to control the risks identified through your risk assessment. While designing your information security program, the Safeguards Rule requires your company to implement the following safeguards controls:



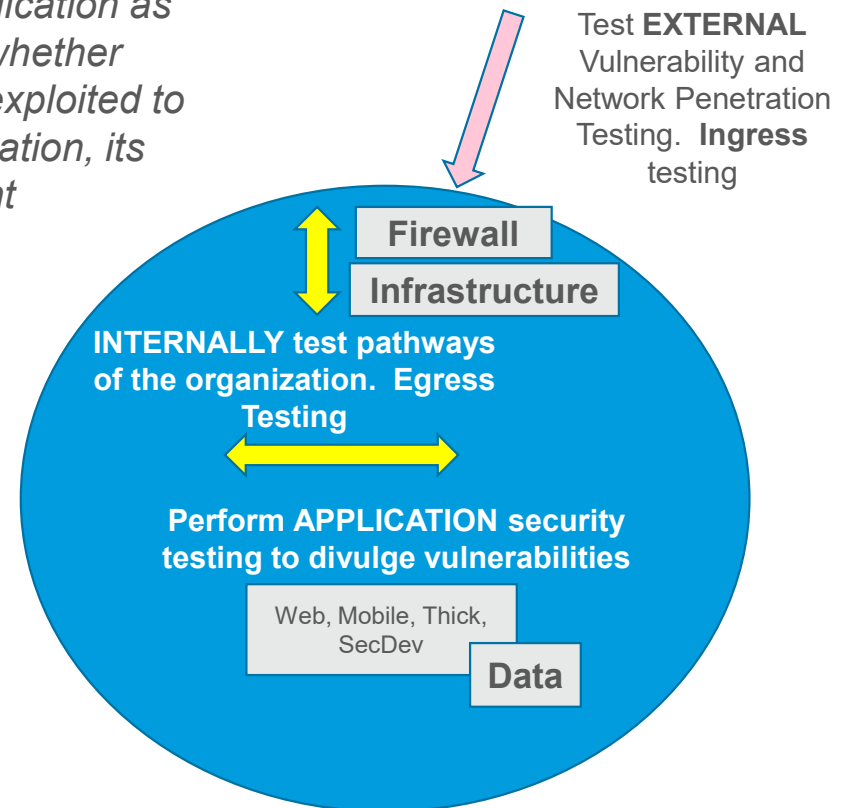
THE PENETRATION TEST MANDATE

- Some form of detection and monitoring effectiveness of controls (not well defined)
- Now, organizations must perform pen tests annually with a vulnerability test at least semi-annually on DEFINED controls. (at a minimum)

A method of testing where testers target individual components of the network or the application as a whole to determine whether vulnerabilities can be exploited to compromise the application, its data, or its environment resources.

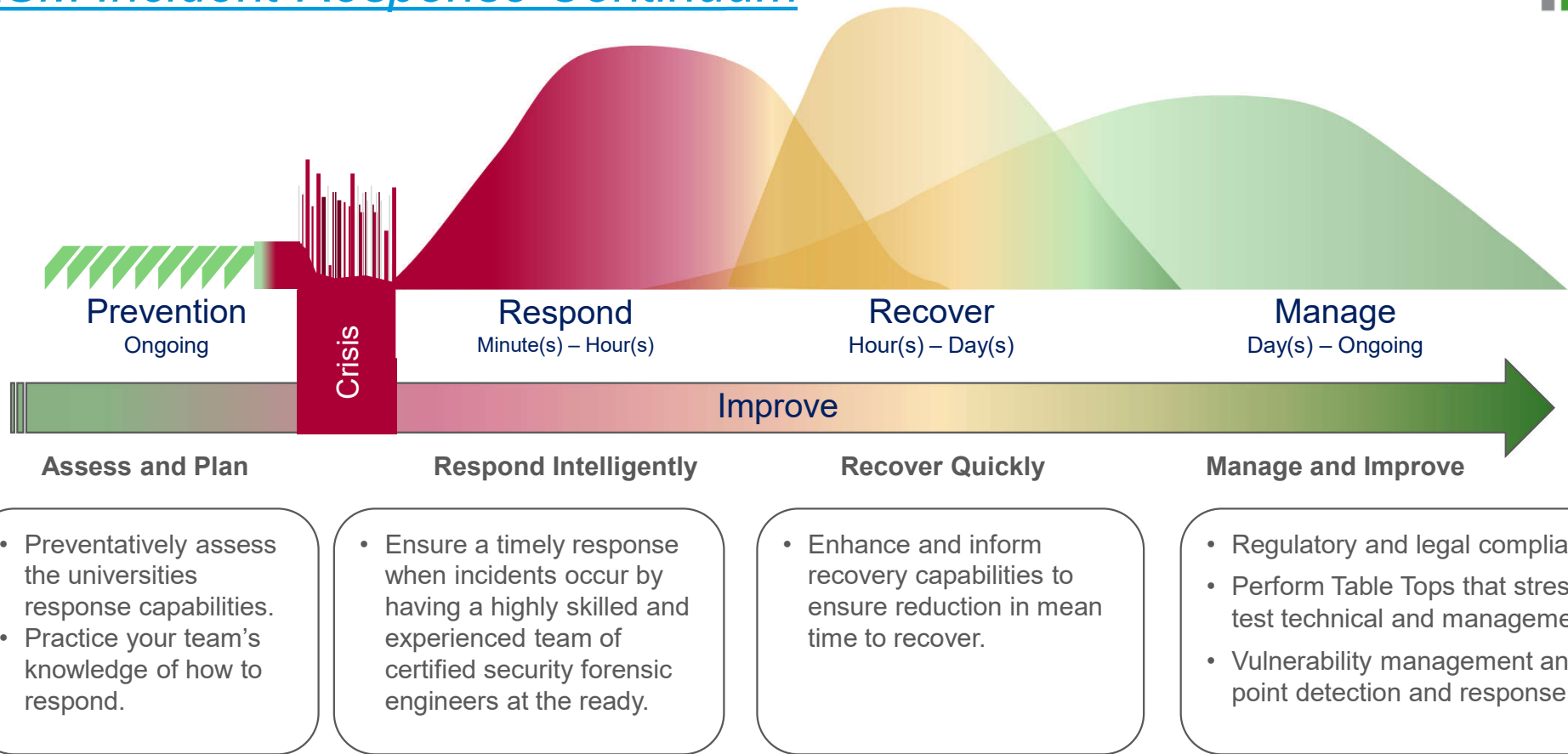
Considerations for H-Ed:

- General Pen Test is a good start...
- Where does SFA Data reside?
- What are the pathways to this data?
- Tied to your Risk Assessment?
- Show gains in maturity...



See slide 17 to see who RSM can assist with Penetration Testing Mandate

RSM Incident Response Continuum



See slide 18 to see who RSM can assist with Prevention and Response

LESSONS LEARNED

Original Deadline of Dec 2022, extended to June, 2023 by the FTC

Lessons Learned from Past Enforcement Actions - **FTC advised companies to:**

- Consider where SFA Data resides, and who has access to this data. (Systems vs. Data view)
- **“Clear and Reasonable” notices** in a manner that consumers are reasonably expected to receive it.
- Document and adjust **information security programs** in light of changes to business operations.
- Report any **data breaches** to the FTC within **10 days** of notifying other government agencies.
- You can outsource services, but **you can’t outsource risk**; maintain your third-party monitoring program.
- Comprehensive, university wide impact: Cross Functional Teams.
- NIST 800.171 framework is the recommended starting point for the DOE.

Polling Question #3

How many days do you have to report a verified breach of SFA Data to the FTC?

- A. 10
- B. 6
- C. 2
- D. 12

RSM UNIVERSE OF SECURITY OFFERINGS

SECURITY PROGRAM MANAGEMENT

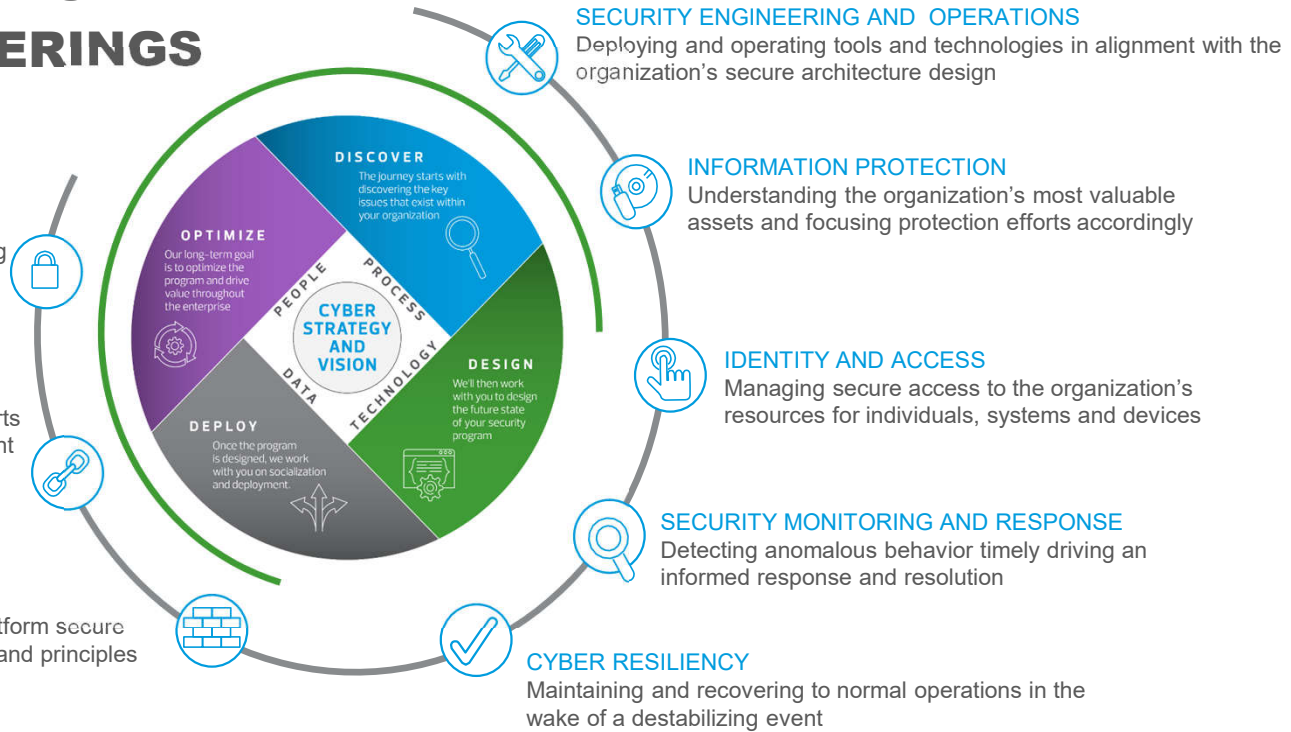
Enabling CISOs to further mature and enhance the capabilities within an organization's cybersecurity program, moving toward operating as a business enabler

RISK AND COMPLIANCE

Guiding alignment of cybersecurity efforts with broader enterprise risk management and compliance obligations

SECURITY ARCHITECTURE

Designing and maturing a cross-platform secure architecture anchored in standards and principles






Are you ready? John and Bob can help!

Register for a free, LITE (1hr) GLBA Readiness Assessment:

Bob.Eckman@rsmus.com discount code: **CACUBO**






RSM CYBER TESTING SERVICES



Services	Description	Offerings	Typical Duration
 Vulnerability Scanning	<ul style="list-style-type: none"> – Automated scanning to identify vulnerabilities due to missing patches, misconfigurations and malicious services – Provides view of vulnerabilities identified without actively exploiting – Can be performed as holistic Vulnerability Management Program 	External Network Internal Network Application	1 – 3 Days
 Network Penetration Testing	<ul style="list-style-type: none"> – Simulated attacks to exploit vulnerabilities to achieve a compromise of sensitive systems and data – Compliance-based if necessary 	External Network Internal Network Wireless Cloud	5 – 10 Days
 Application Security	<ul style="list-style-type: none"> – Penetration testing focused on an application including testing the business logic and flow of the application – Static and Dynamic scanning options available 	Web Applications Mobile (iOS & Android) Thick Client Secure Dev. Training	5 – 10 Days
 Red/Purple Teaming	<ul style="list-style-type: none"> – In-depth technical testing using selected tactics actual threat actors would use to evade detection and exfiltrate data – Targets certain trophies – Goal is to test monitoring, detection and response capabilities 	Red Teaming Purple Teaming	8 – 12 Weeks
 Social Engineering	<ul style="list-style-type: none"> – Test an organization's security awareness and alignment to existing security policies – Use deception to coerce a user in providing access or information that could be leveraged to access a system 	Email (Phishing) Phone Call (Vishing) Text Message (SMSing) In-Person	3 – 5 Days

RSM CYBER INCIDENT RESPONSE SERVICES



Services	Description	Offerings	Typical Duration
 Incident Response Proactive Services:	<ul style="list-style-type: none"> – RSM Incident Response Planning (IRP) can build, review, update your IR Plans – Train your staff to an industry standard IR approach. – Help you to establish and/or train your incident response team 	Incident Response Evaluation – Tools, personnel, plans	5 to 6 Weeks
 Incident Response Table Tops	<ul style="list-style-type: none"> – Exercise your team’s knowledge and skills. – Customized, simulated attacks to exploit vulnerabilities to achieve a compromise of sensitive systems and data – Compliance-based to test specific controls (HIPAA, GLBA, etc..) 	Technical Table Top Management Table Top Ransomware Table Top	5 to 6 Weeks
 Incident Response Retainer Services	<ul style="list-style-type: none"> – A team of highly skilled and experienced cyber forensic professionals at the ready. – Can act as your response team OR compliment your response team – Can help to educate your teams on response – <i>Unused funds can be used towards other cyber security initiatives.</i> 	Yearly On Call Monthly On Call Advisory Services	Annual Monthly Ad hoc
 “Phone a Friend” Services	<ul style="list-style-type: none"> – Experienced response and resiliency consultants to advise and provide unbiased inputs. – Can inform and advise relative to governance, risk, and compliance. – Can mentor and guide your information security staff 	IR Advisory Services Resiliency Consulting	Immediate Ad Hoc
 Business Continuity and Disaster Recovery	<ul style="list-style-type: none"> – Review/update/establish business continuity programming documentation. – Review Business Impact Analysis – Establish recovery pathways and redundancies for critical applications – Provide crisis as well as cyber response management 	Business Continuity Planning Response, Recovery, and Remediation	10 to 12 Weeks Immediate/Ad hoc

Polling Question #4

Was this information helpful to better understand the GLBA regulation and how it applies to Higher Education?

- A. Yes
- B. No
- C. Maybe



TENTATIVE UPCOMING CACUBO PROGRAMMING



- Feb. 16 – Webinar – Equitable Access: Ditching Print Textbooks While Improving Student Outcomes - Follett
- March 22 – Webinar – GASB Update - Plante Moran
- April 13 – Webinar – Ethics - Rubin Brown
- Late March/Early April – Drive In Workshop in or around Des Moines, Iowa
- May 7-10 – Accounting and Business Operations Workshop - Louisville
- May 18 – Webinar – Accounting 101 for Colleges and Universities – Baker Tilly
- August 7-8 – Women’s Leadership Institute - Milwaukee
- October 1 – 3 – Annual Conference – Omaha

THANK YOU FOR
YOUR TIME AND
ATTENTION



www.rsmus.com

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party.

For more information, visit rsmus.com/who-we-are for more information regarding RSM US LLP and RSM International.

© 2023 RSM US LLP. All Rights Reserved.

