CLARK SCHAEFER HACKETT
BUSINESS ADVISORS

2024 Cybersecurity Update

What Financial Professionals in the Public Sector Should Know About Cybersecurity

Presented by:

Carly Devlin & Ross Patz

CLARK SCHAEFER
CONSULTING

Speakers

Carly Devlin
Shareholder, IT Risk and Cybersecurity Practice

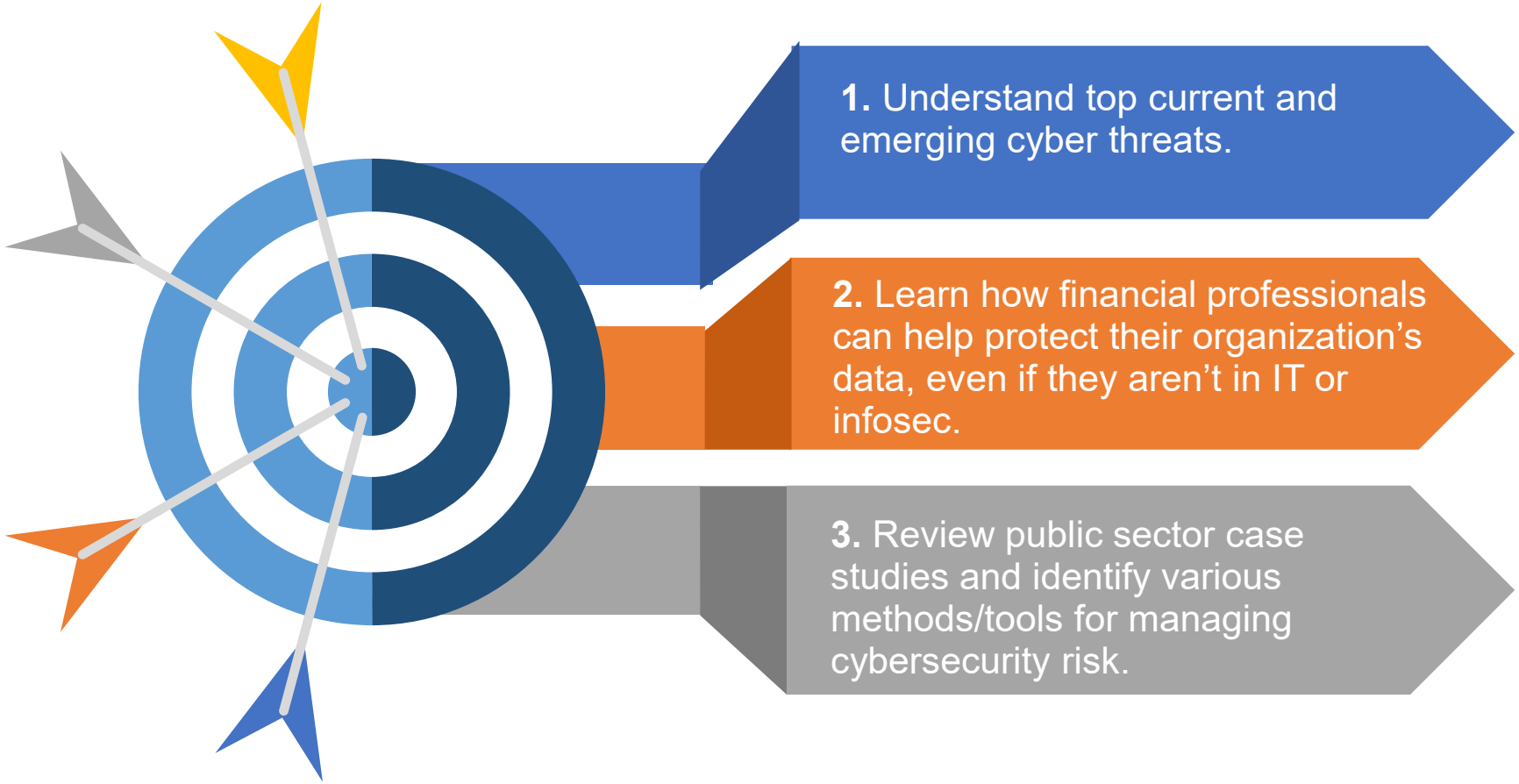
Chief Information Security Officer

- Shareholder at Clark Schaefer Hackett leading the firm's IT Risk and Cybersecurity consulting practice
- CSH Chief Information Security Officer, turning her focus internally to help guide the firm's cybersecurity strategy.
- Background in Fortune 500 companies like JPMorgan Chase and Progressive Insurance.
- Certified Information Systems Auditor (CISA) and Certified Information Systems Security Professional (CISSP)
- Her clients appreciate her ability to provide practical recommendations, guide them through complex security and risk management issues, and help them achieve their goals with confidence.

Ross Patz
Director, IT Risk and Cybersecurity Practice

- Director at Clark Schaefer Hackett in the IT Risk and Cybersecurity consulting practice
- Currently advancing his expertise by pursuing a Ph.D. in Cyber Defense at Dakota State University.
- Grant-funded researcher and a member of PriLab at the university where he contributes to research in privacy and cybersecurity.
- Certified Ethical Hacker (CEH) and Computer Hacking Forensic Investigator (CHFI)
- His combination of practical experience, technical prowess, and academic rigor make him a valuable asset, not only in his current role but also in the broader IT and cybersecurity community.

Objectives



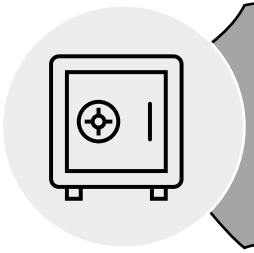
1. Understand top current and emerging cyber threats.

2. Learn how financial professionals can help protect their organization's data, even if they aren't in IT or infosec.

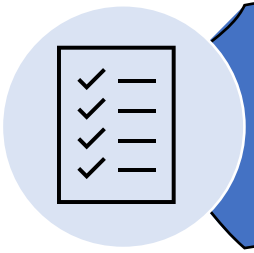
3. Review public sector case studies and identify various methods/tools for managing cybersecurity risk.

Agenda

1. Current State of Cybersecurity



2. The Financial Professional's Role in Cybersecurity



3. Recent Public Sector Attacks & Managing Cyber Risk

Current State of Cybersecurity

Threats Are Ever Changing…

- **93%** of respondents report that line-of-business end users rely on generative AI tools to help them do their jobs. But **65%** admit they lack education around generative AI and **34%** lack a complete generative AI policy.
- **48%** of security leaders have experienced cyber extortion, making it a more common cyberattack in 2024 than ransomware.

Source: Splunk State of Security Report

Top Trends

1. **Generative AI**
2. Cybersecurity Metrics
3. Security Behavior & Culture Programs
4. Efficient Third Party Risk Management
5. Continuous Threat Exposure Management Programs
6. Extending the Role of Identity & Access Management

Top Trends: Generative AI

Generative AI: artificial intelligence capable of generating text, images, videos, or other data using generative models, often in response to prompts. Generative AI models learn the patterns and structure of their input training data and then generate new data that has similar characteristics.

- Innovation vs. security
- Cross-functional governance is key
- AI cybersecurity use cases
- Solving the cyber skills shortage
- AI as a tool for adversaries

Top Trends

1. Generative AI
2. **Cybersecurity Metrics**
3. Security Behavior & Culture Programs
4. Efficient Third Party Risk Management
5. Continuous Threat Exposure Management Programs
6. Extending the Role of Identity & Access Management

Top Trends: Cybersecurity Metrics

Outcome-driven metrics (ODMs): Measure the outcomes of security investments

- Traditional metrics can fall short
- ODMs provide a credible and defensible expression of risk appetite that supports direct investment to change protection levels
- Use simple language that is explainable to non-IT execs

Top Trends

1. Generative AI
2. Cybersecurity Metrics
3. **Security Behavior & Culture Programs**
4. Efficient Third Party Risk Management
5. Continuous Threat Exposure Management Programs
6. Extending the Role of Identity & Access Management

Top Trends: Security Behavior & Culture Programs

Security Behavior & Culture Programs: Enterprise-wide approach to minimizing cybersecurity incidents associated with employee behavior.

- Shifting focus from awareness to fostering behavioral change
- By 2027, 50% of large enterprise CISOs will adopt human-centric security design practices to minimize cyber-induced friction and maximize control adoption.

Top Trends

1. Generative AI
2. Cybersecurity Metrics
3. Security Behavior & Culture Programs
4. **Efficient Third Party Risk Management**
5. Continuous Threat Exposure Management Programs
6. Extending the Role of Identity & Access Management

Top Trends: Efficient Third Party Risk Management

Third Party Risk Management: Inevitability of third parties experiencing cyber incidents is pressuring security leaders to focus more on resilience-oriented investments and move away from front loaded due diligence activities.

- Strengthen contingency plans for third-parties that pose the highest cyber risk
- Create third-party specific incident playbooks
- Define a clear offboarding strategy

Top Trends

1. Generative AI
2. Cybersecurity Metrics
3. Security Behavior & Culture Programs
4. Efficient Third Party Risk Management
5. **Continuous Threat Exposure Management Programs**
6. Extending the Role of Identity & Access Management

Top Trends: Continuous Threat Exposure Management Programs

Continuous Threat Exposure Management: systemic approach used to continually evaluate the accessibility, exposure, and exploitability of digital and physical assets.

- Align assessment scope with threat vectors or projects rather than infrastructure components
- Can be used to continuously monitor hybrid digital environments to enable early identification of vulnerabilities

Top Trends

1. Generative AI
2. Cybersecurity Metrics
3. Security Behavior & Culture Programs
4. Efficient Third Party Risk Management
5. Continuous Threat Exposure Management Programs
6. **Extending the Role of Identity & Access Management**

Top Trends: Extending the Role of Identity & Access Management

Identity & Access Management: Framework of policies and technologies to ensure that the right users have the appropriate access to technology resources.

- IAM's role in cyber has been increasingly steady
- Focus shifts from network security and other traditional controls to IAM in an identify-first approach to security

Poll Question #1

Of these top trends we discussed today, which do you feel will be most important for your organization to focus on?

a) Generative AI
b) Cybersecurity Metrics
c) Security Behavior & Culture Programs
d) Efficient Third Party Risk Management
e) Continuous Threat Exposure Management Programs

Public Sector Trends

For state and local governments, malware attacks increased from 2022 to 2023 by 148%, ransomware incidents were up 51%, and non-malware attacks were up 37%.

Source: Center for Internet Security

Cybersecurity should be a top concern for state and local governments!

Top Public Sector Threats

76% of cybersecurity incidents in the public sector resulted from…

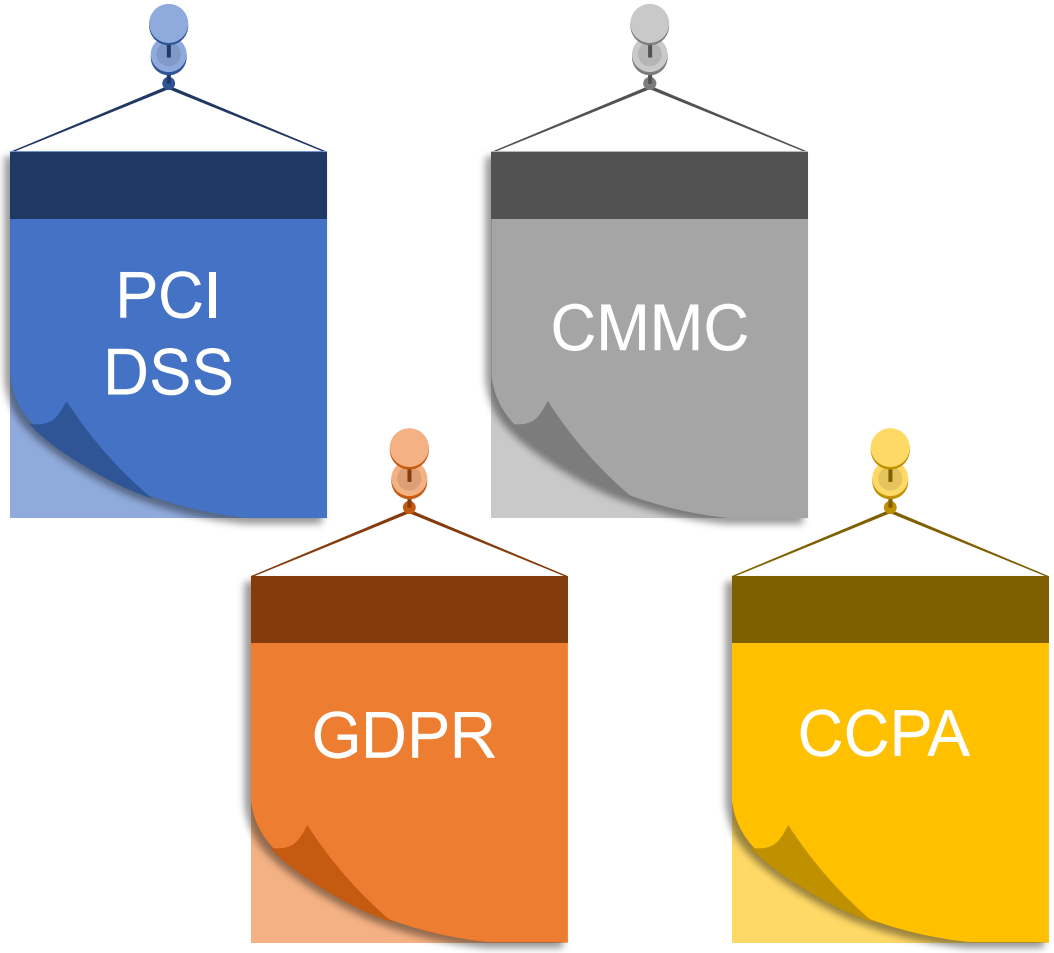
1. System intrusion
2. Lost and stolen assets
3. Social engineering attacks

Source: 2023 Verizon Data Breach Report

Why Public Sector Entities Targeted?

1. Outdated technology, software, and legacy systems with known vulnerabilities
2. Smaller cyber budgets
3. Limitations in IT staffing and resources
4. Outsourcing of IT services

Current Regulatory Landscape



CURRENTLY: The U.S. has no comprehensive national cybersecurity law.

Upcoming Changes in the Regulatory Landscape

New cybersecurity regulations are coming!

Poll Question #2

Do you feel your organization experiences the issues that cause state and local governments to be targeted by cyber attacks?

a. Yes
b. No
c. I'm not sure

The Financial Professional's Role in Cybersecurity

Know the “Crown Jewels”

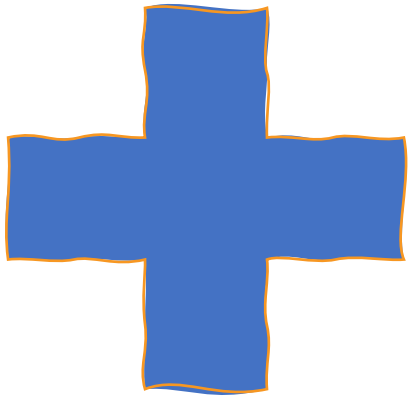
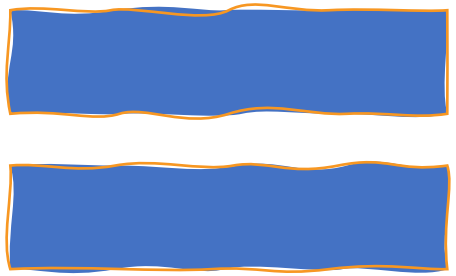
Crown Jewels: Data without which your business would have difficulty operating and/or the information that could be a high-value target for cybercriminals.

Source: National Cybersecurity Alliance

Example “Crown Jewels”

- Vendor lists
- Customer lists
- Inventory
- Payments history
- Receivables
- Contracts/service agreements
- Employee records

Protect the “Crown Jewels”

Finance  Cybersecurity 

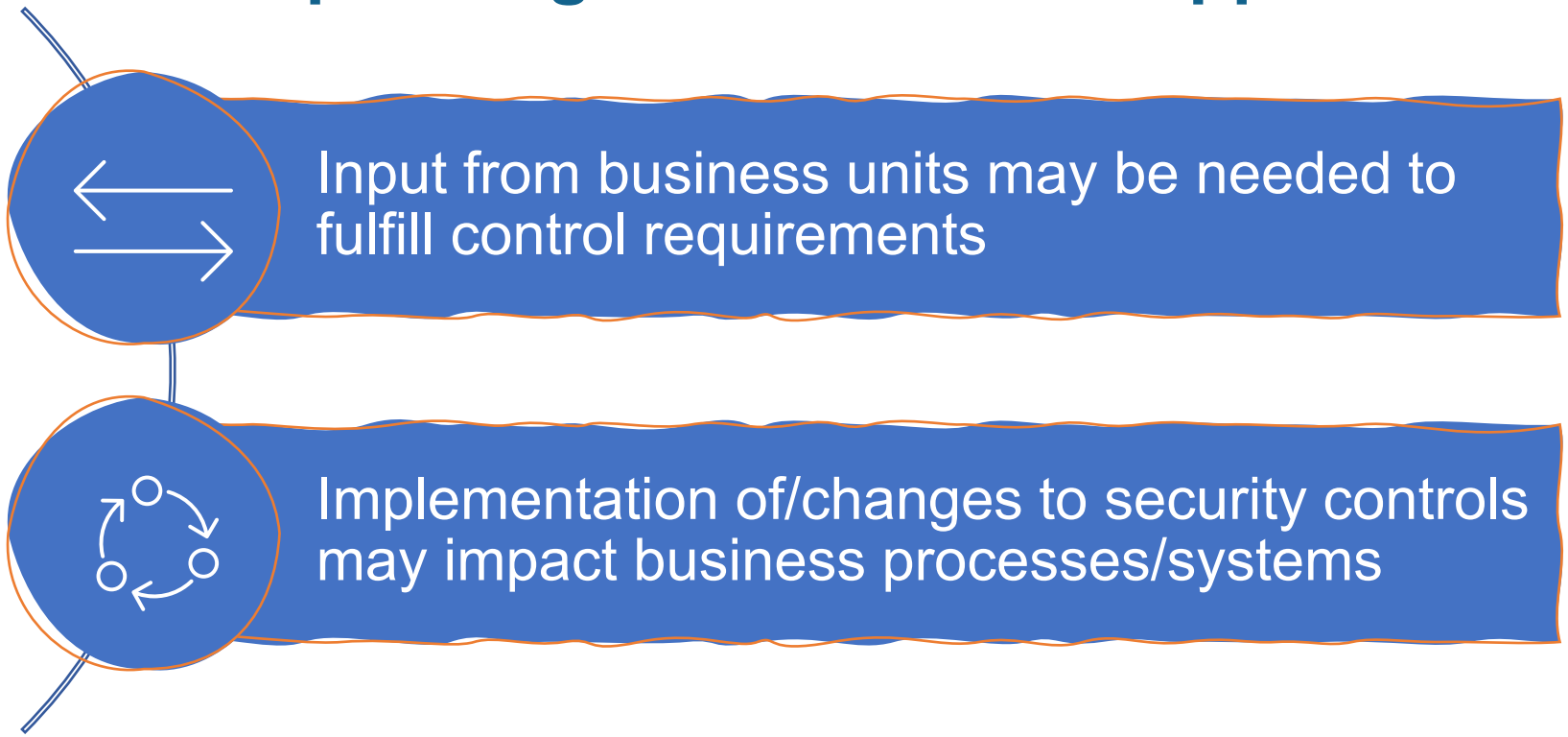
Better Protection of Crown Jewels

Participate in/Champion Organizational Initiatives

- ✓ Compliance (e.g. PCI)
- ✓ Business Impact Analysis
- ✓ Data Governance
- ✓ Incident Response

Compliance Initiatives

All security related compliance initiatives require organization-wide support.



Compliance Initiatives – Examples

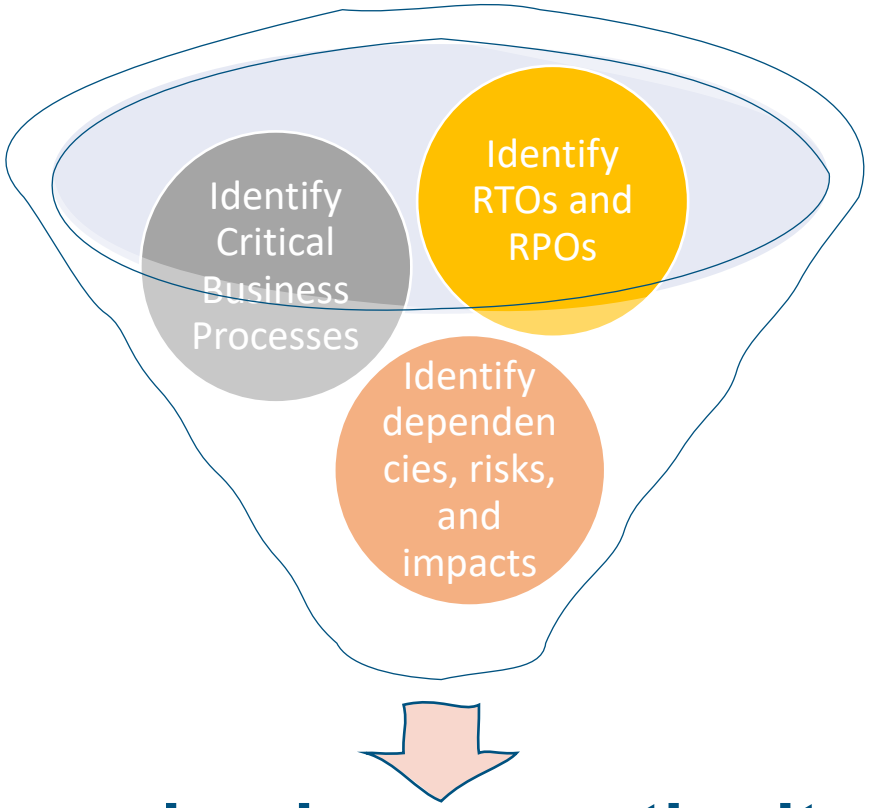
PCI Security Standards Council

Requirements and Testing Procedures	
7.2 Access to system components and data is appropriately defined and assigned.	
Defined Approach Requirements	**Defined Approach Testing Procedures**
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	**7.2.1.a** Examine documented policies and procedures and interview personnel to verify the access control model is defined in accordance with all elements specified in this requirement. **7.2.1.b** Examine access control model settings and verify that access needs are appropriately defined in accordance with all elements specified in this requirement.

PCI Security Standards Council

Requirements and Testing Procedures	
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	
Defined Approach Requirements	**Defined Approach Testing Procedures**
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	**12.8.1.a** Examine policies and procedures to verify that processes are defined to maintain a list of TPSPs, including a description for each of the services provided, for all TPSPs with whom account data is shared or that could affect the security of account data.
Customized Approach Objective	**12.8.1.b** Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.
Records are maintained of TPSPs and the services provided.	
Applicability Notes	
The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.	

Business Impact Analysis



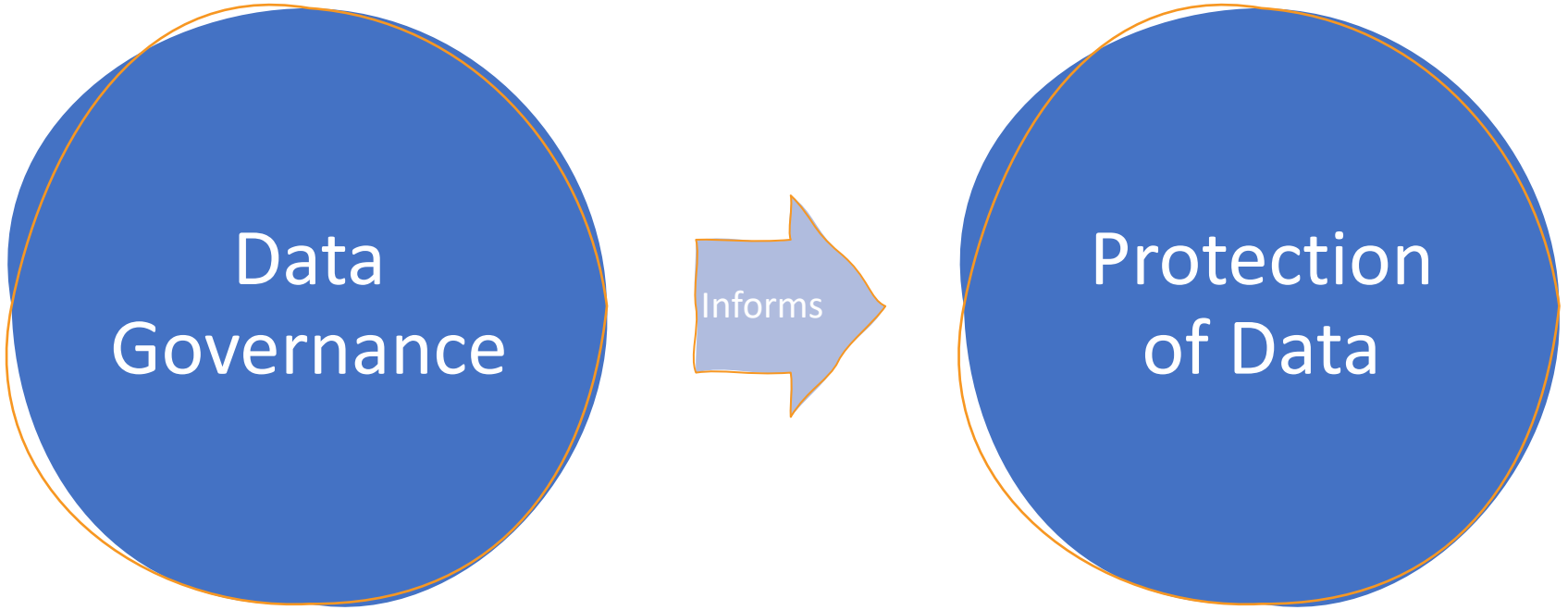
Informs business continuity and disaster recovery activities

Business Impact Analysis

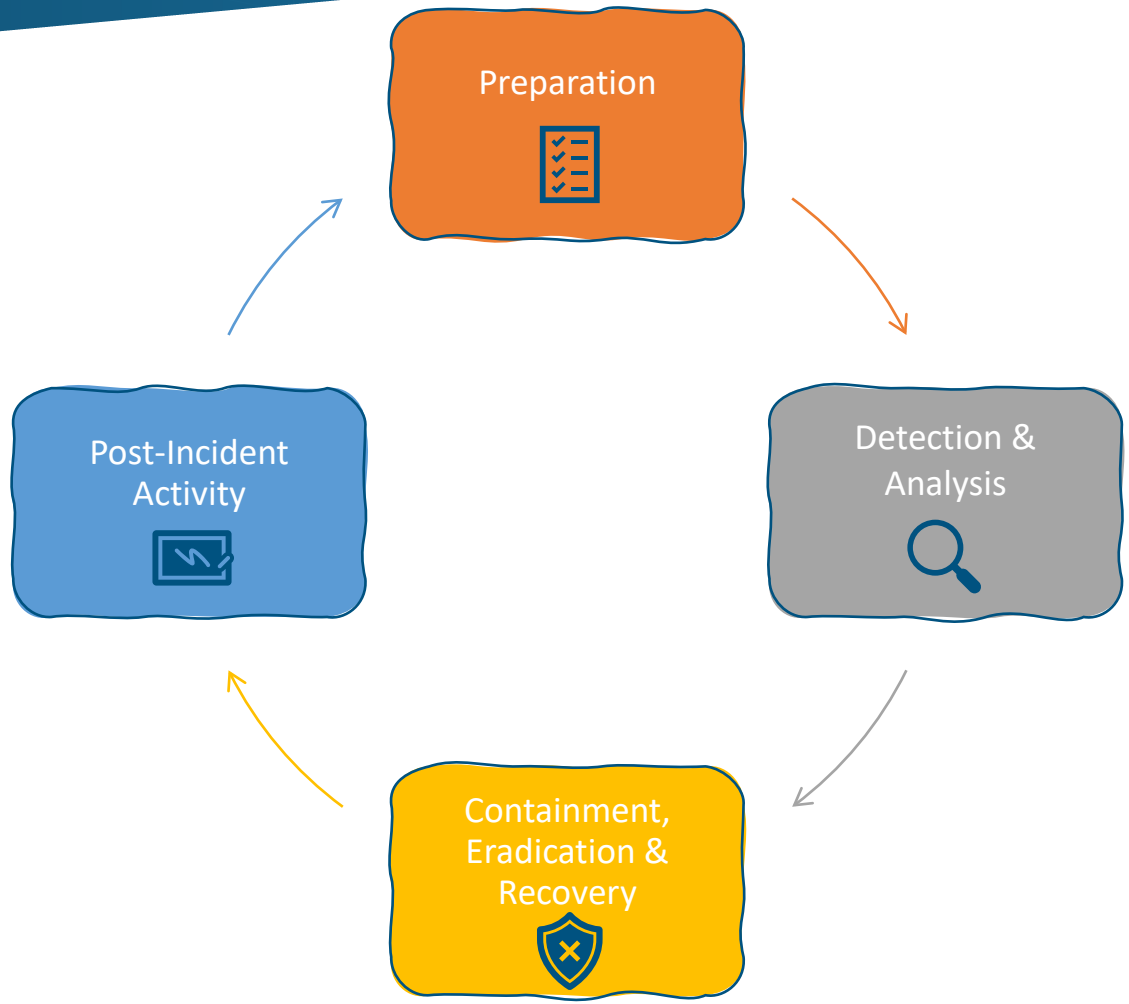
Function	Category	Subcategory
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)

Function	Category	Subcategory
		PR.IP-8: Effectiveness of protection technologies is shared
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10: Response and recovery plans are tested

Data Governance



Know Your Role in Incident Response



Senior Leadership Tabletop Exercises

Interactive, discussion-based exercise focused on an organization's response to a security incident. Potential topics:

Poll Question #3

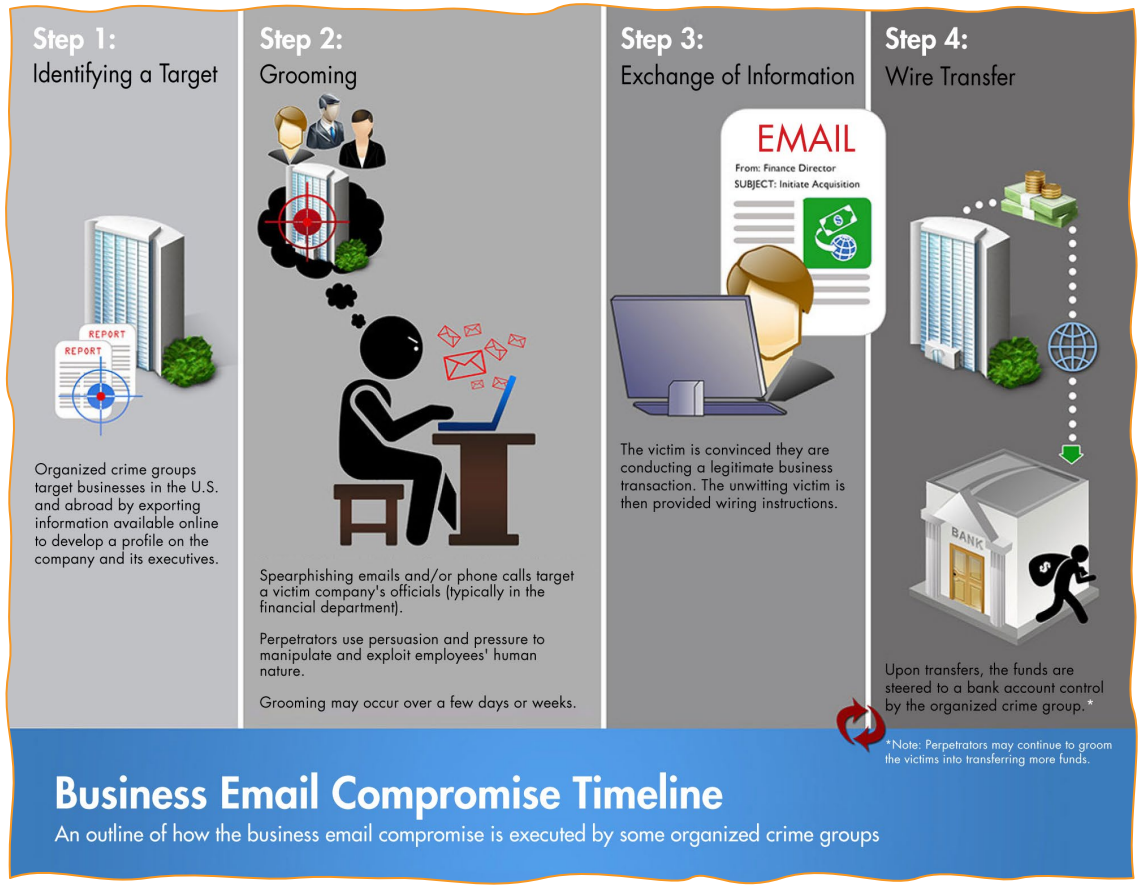
Have you been involved in working with IT/security on any of the initiatives we've discussed today?

a. Yes
b. No
c. I'm not sure

Be Aware of Common Schemes

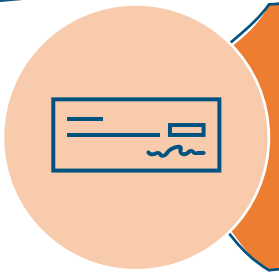
BEC: Business Email Compromise

Criminals send an email message that appears to come from a known source making a legitimate request.



Source: FBI

BEC Scenarios



A familiar vendor sends an invoice with an updated mailing address.

CEO asks her assistant to purchase dozens of gift cards.

Homebuyer receives a message from title company with instructions for wiring down payment

Source: FBI

How Criminals Carry Out BEC Scams

A scammer might:

- **Spoof an email account or website**

  Slight variation on legitimate email address

- **Send spearphishing emails**

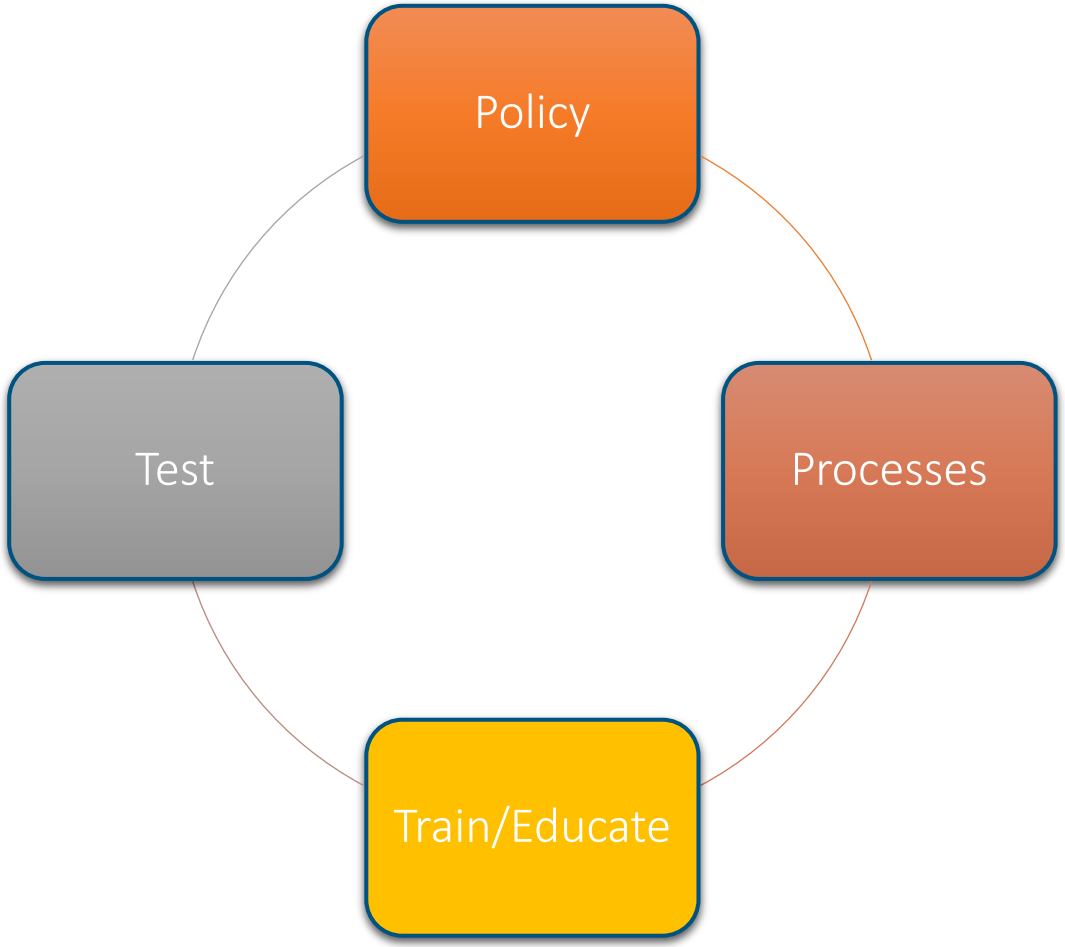
  Looks like it's from a trusted sender

- **Use malware**

  Malicious software that can gain access to legitimate email threads

Source: FBI

BEC Prevention Tips



Don’t Fall for BEC Scams

Be careful what you share on social media.

Don’t click on anything in an unsolicited email or text.

Carefully examine email address, URL, and spelling in emails.

Don’t open attachments from anyone you don’t know.

Source: FBI

Poll Question #4

Do you feel there is a strong awareness of Business Email Compromise scenarios within your organization?

a. Yes
b. No
c. I’m not sure

Recent Public Sector Attacks

Recent Public Sector Attacks

1. Fulton County, GA
2. Bucks County, PA
3. Kansas City Area Transportation Authority
4. Oakley, CA
5. Business Email Compromise (BEC) Attacks

Fulton County, GA

- **When:** January 2024
- **What:** Phone lines and many systems were taken down for weeks
- **How:** Ransomware group LockBit 3.0 took credit for the attack and threatened to release residents' personal information online.

Bucks County, PA

- **When:** January 2024
- **What:** Knocked out Emergency Communications' Department's computer-aided dispatch system for 9 days
- **How:** Officials believe ransomware group Akira was responsible for the attack

Kansas City Area Transportation Authority

- **When:** January 2024
- **What:** Ransomware attack resulting in ongoing communication disruptions
- **How:** The Medusa ransomware group claimed responsibility for the attack and has published samples of the alleged stolen data

Oakley, CA

- **When:** February 2024
- **What:** A ransomware attack resulted in several systems being taken offline, causing delays in city government services.

Business Email Compromise Attacks

- **When:** 2024
- **What:** A hacking group known as TA4903 has been impersonating US government agencies, including the Department of Transportation, Department of Agriculture and Small Business Administration
- **How:** They trick targets into opening malicious files using QR codes in PDF attachments designed to resemble the spoofed organization.

Managing Cybersecurity Risk

Compliance vs. Risk Management

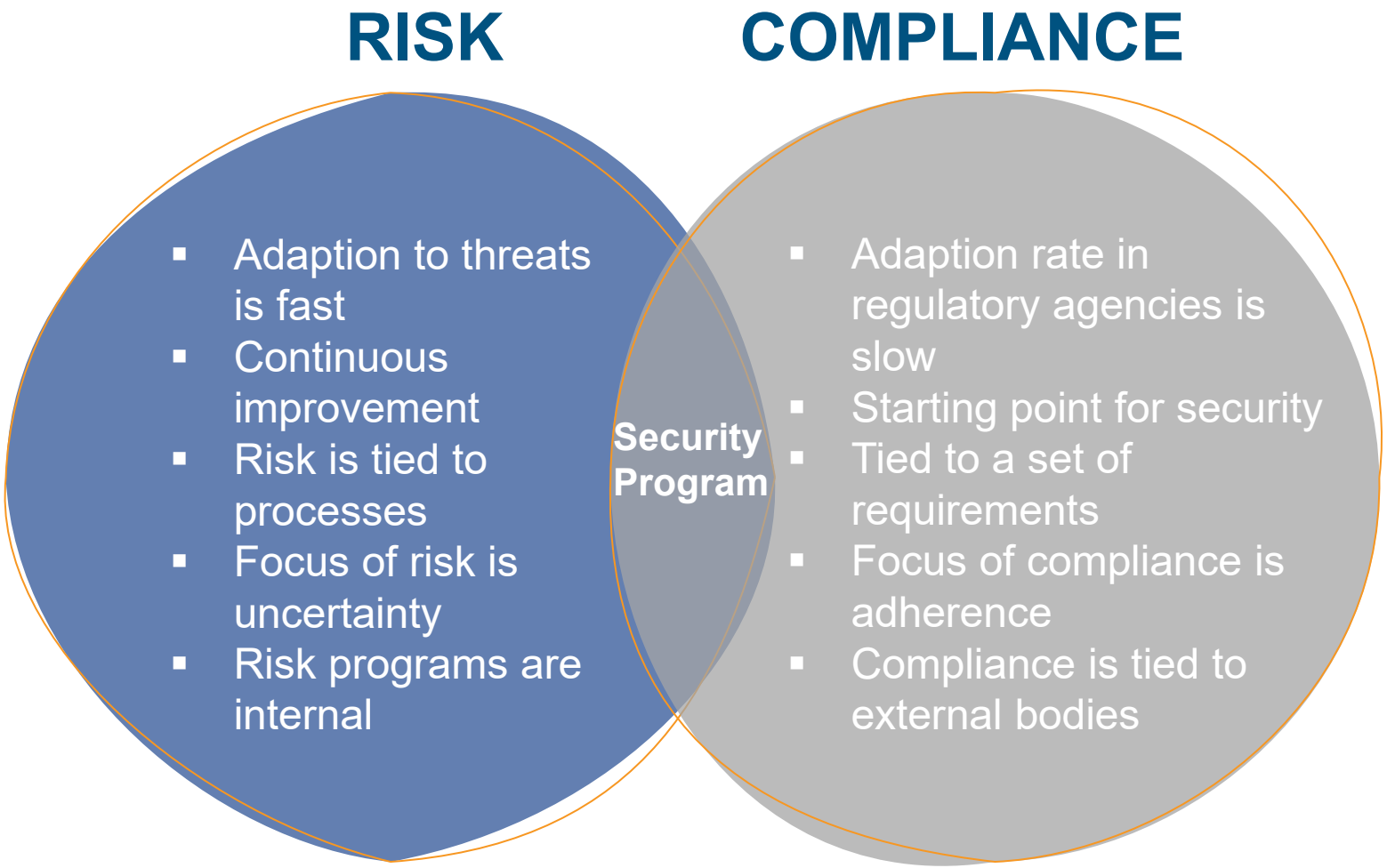
COMPLIANCE

Prescriptive, tactical, check-the-box

RISK MANAGEMENT

Predictive, anticipatory, strategic

Compliance vs. Risk Management

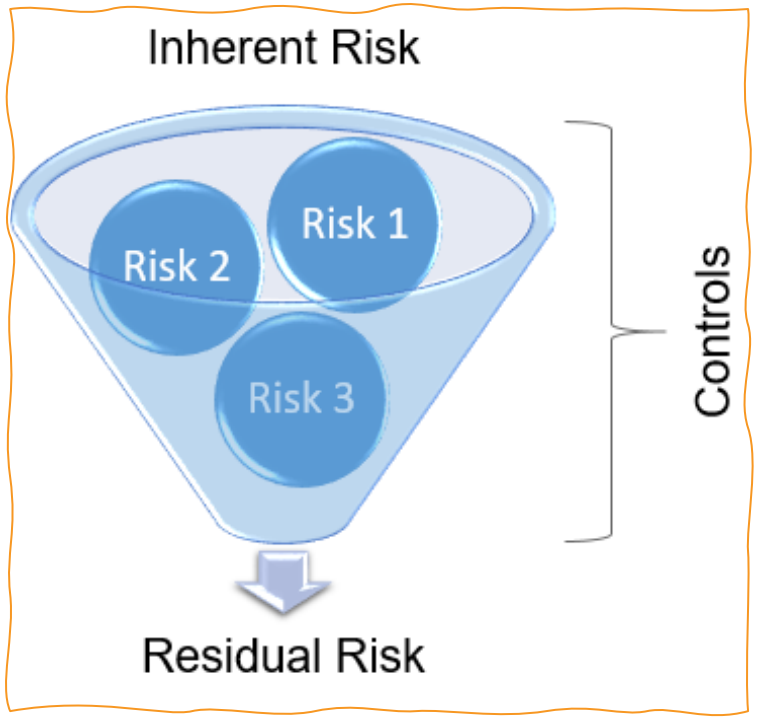


Security Risk Management Concepts/Best Practices

- Take a **risk-based approach**
- Develop a cybersecurity risk management **strategy**
- Adopt a cybersecurity risk management **framework**
- Don’t stop at **compliance**
- Implement **defense-in-depth**
- Apply **metrics** to measure effectiveness
- Test your **incident response** and **disaster recovery** plans

Risk Assessment

- All information security activities should be based on risk assessment
- Threats/risks vary from organization to organization
- Based on identified risks, the appropriate level of control can be implemented



Security Frameworks

NIST 800-53
NIST Cybersecurity Framework

CIS Controls

ISO 27001/2

Negative Effects of Poor Risk Management

- Inability to **secure funding** for cybersecurity initiatives
- Inability to **prioritize** cybersecurity initiatives
- **Reputational damage** in the event of a security incident
- **Financial loss** due to fines and/or lost revenue

Poll Question #5

Does your organization focus more on risk management or compliance when it comes to cybersecurity?

a. More focus on compliance
b. More focus on risk management
c. The focus is balanced
d. I’m not sure

Key Takeaways

- The current cybersecurity threat and regulatory landscape is changing rapidly.
- Financial professionals also have responsibility to assist with and promote cybersecurity initiatives.
- Continued awareness of threats and common schemes is imperative for financial professionals.
- Both risk management and compliance comprise an effective security program.

CLARK SCHAEFER HACKETT
BUSINESS ADVISORS

QUESTIONS?

CLARK SCHAEFER
CONSULTING