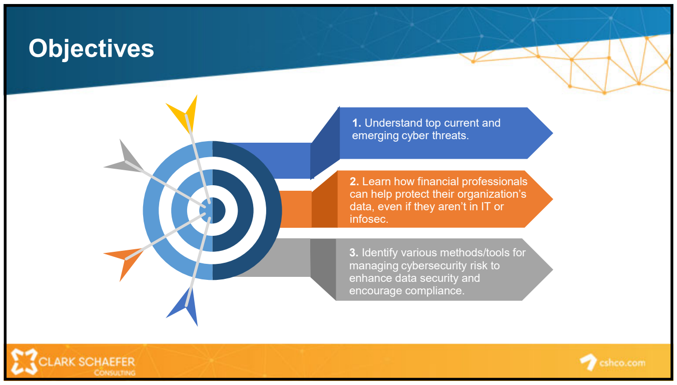
CLARK SCHAEFER HACKETT
BUSINESS ADVISORS

Cybersecurity Trends in 2022

What Accountants in the Public Sector Should Know About Cybersecurity

Presented by:
Carly Devlin

CLARK SCHAEFER
CONSULTING



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. Identify various methods/tools for managing cybersecurity risk to enhance data security and encourage compliance.

CLARK SCHAEFER CONSULTING

cshco.com

Agenda

1. Current State of Cybersecurity
2. The Financial Professional's Role in Cybersecurity
3. Managing Cybersecurity Risk

CLARK SCHAEFER CONSULTING

cshco.com

Current State of Cybersecurity

CLARK SCHAEFER CONSULTING

cshco.com

Threats Are Ever Changing…

- 60% of knowledge workers are remote, and at least 18% will not return to the office.
- By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

Source: Gartner

CLARK SCHAEFER CONSULTING

cshco.com

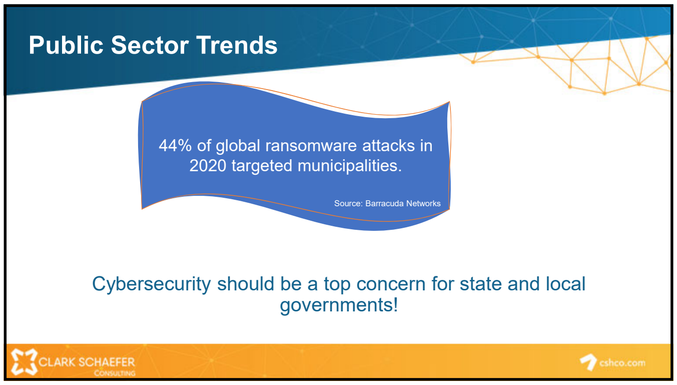
Top Trends

Gartner Says:

1. Attack surface expansion
2. Identity system defense
3. Digital supply chain risk
4. Vendor consolidation
5. Cybersecurity mesh
6. Distributed decisions
7. Beyond awareness

CLARK SCHAEFER CONSULTING

cshco.com

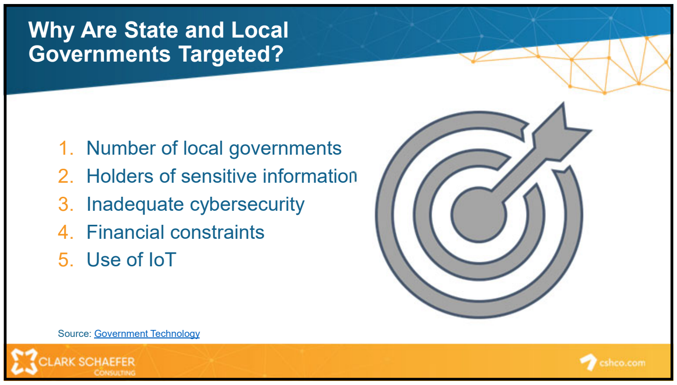


Public Sector Trends

44% of global ransomware attacks in 2020 targeted municipalities.

Source: Barracuda Networks

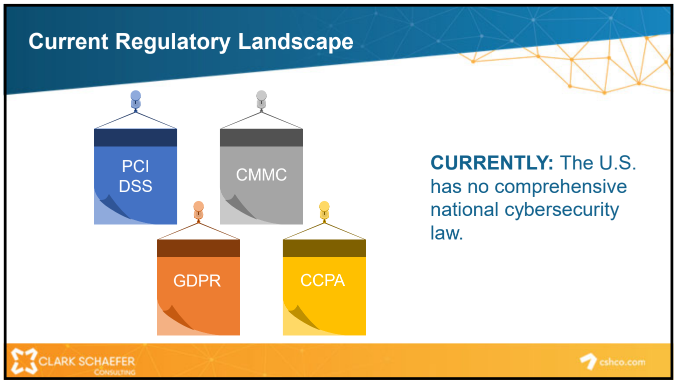
Cybersecurity should be a top concern for state and local governments!



Why Are State and Local Governments Targeted?

1. Number of local governments
2. Holders of sensitive information
3. Inadequate cybersecurity
4. Financial constraints
5. Use of IoT

Source: Government Technology



Current Regulatory Landscape

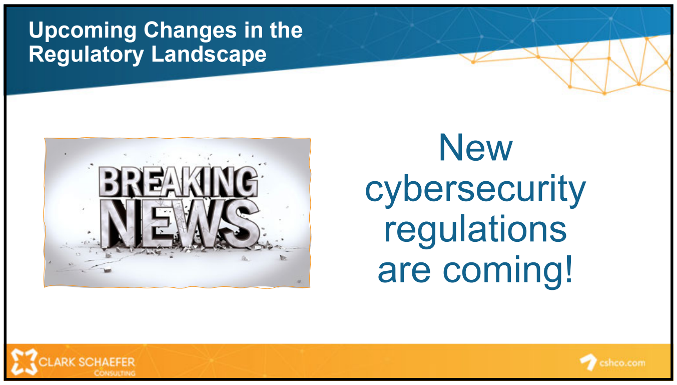
PCI DSS

CMMC

GDPR

CCPA

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


BREAKING NEWS

Upcoming Changes in the Regulatory Landscape

New cybersecurity regulations are coming!

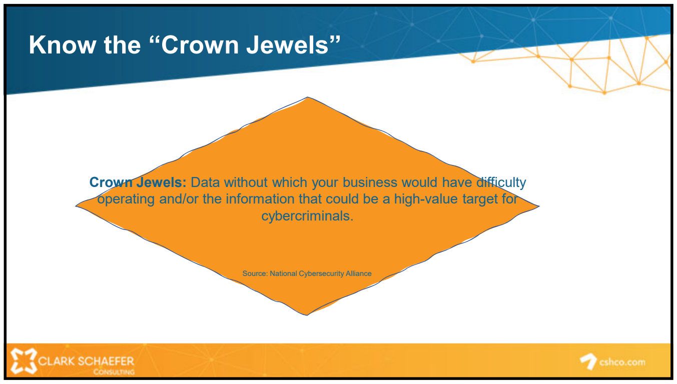
CLARK SCHAEFER CONSULTING

cshco.com

The Financial Professional's Role in Cybersecurity

CLARK SCHAEFER CONSULTING

cshco.com



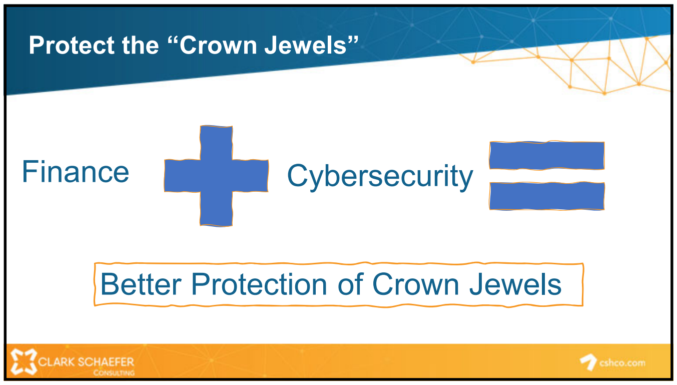
Know the "Crown Jewels"

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

CLARK SCHAEFER CONSULTING

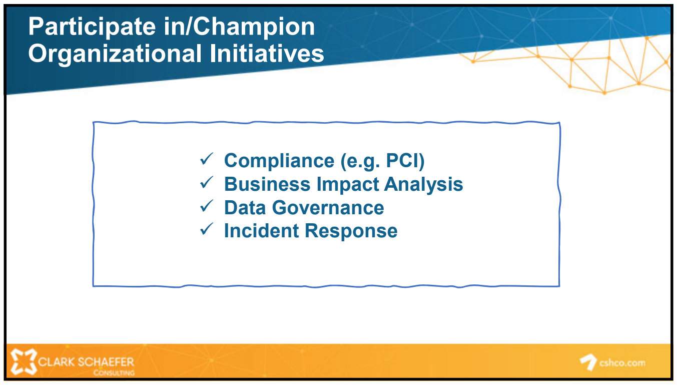
cshco.com



Protect the "Crown Jewels"

Finance + Cybersecurity =

Better Protection of Crown Jewels



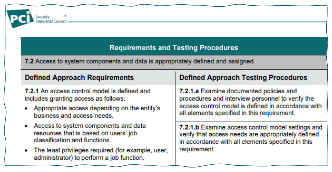
Participate in/Champion Organizational Initiatives

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

Compliance Initiatives

All security related compliance initiatives require organization-wide support.

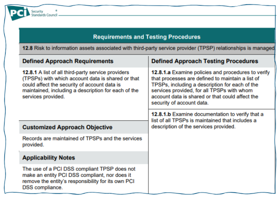
Compliance Initiatives – Examples



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.



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. **12.8.1.b** Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.

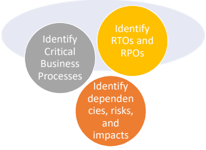
Customized Approach Objective

Records are maintained of TPSPs and the services provided.

Applicability Notes

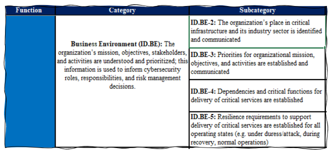
The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.

Business Impact Analysis

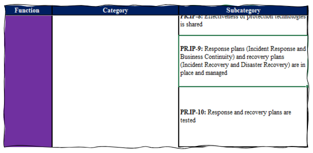

Identify Critical Business Processes
Identify RTOs and RPOs
Identify dependencies, risks, and impacts

Informs business continuity and disaster recovery activities

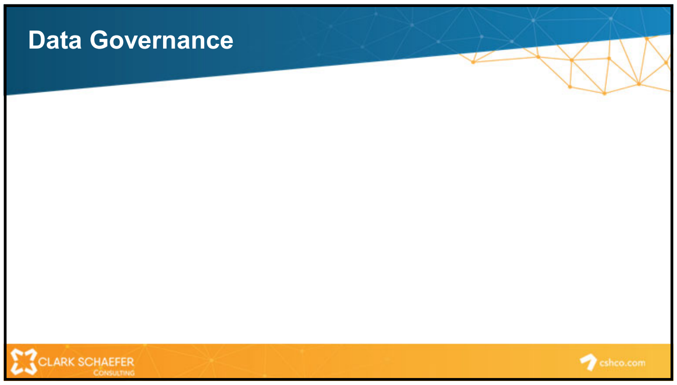
Business Impact Analysis



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)

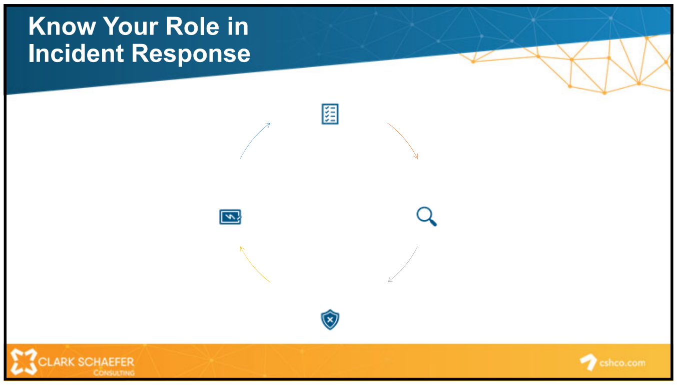


Function	Category	Subcategory
		PR.IP-8: Effectiveness of protection technologies is shared
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10: Response and recovery plans are tested

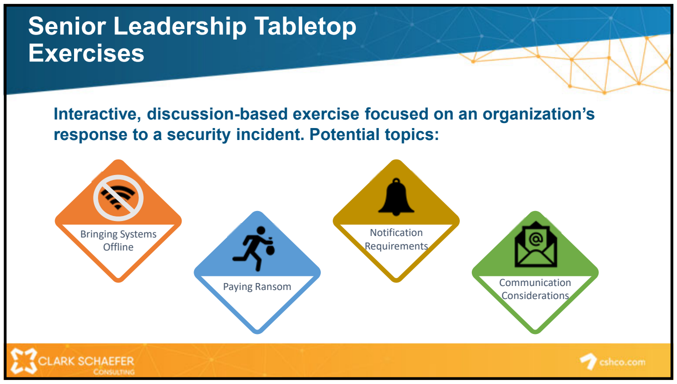


Data Governance

CLARK SCHAEFER CONSULTING
cshco.com



Know Your Role in Incident Response



Senior Leadership Tabletop Exercises

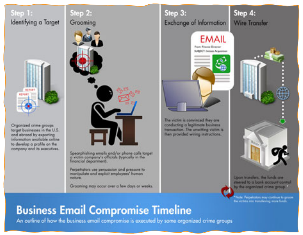
Interactive, discussion-based exercise focused on an organization's response to a security incident. Potential topics:

Bringing Systems Offline
Paying Ransom
Notification Requirements
Communication Considerations
CLARK SCHAEFER CONSULTING
cshco.com

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.



Step 1: Identifying a Target

Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2: Grooming

Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information

The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer

Upon transfers, the funds are steered to a bank account control by the organized crime group.*

*Note: Perpetrators may continue to groom the victims into transferring more funds.

Business Email Compromise Timeline

An outline of how the business email compromise is executed by some organized crime groups

Source: FBI

BEC Scenarios

Source: FBI

How Criminals Carry Out BEC Scams

A scammer might:

- **Spoof an email account or website**

  Slight variation on legitimate email address

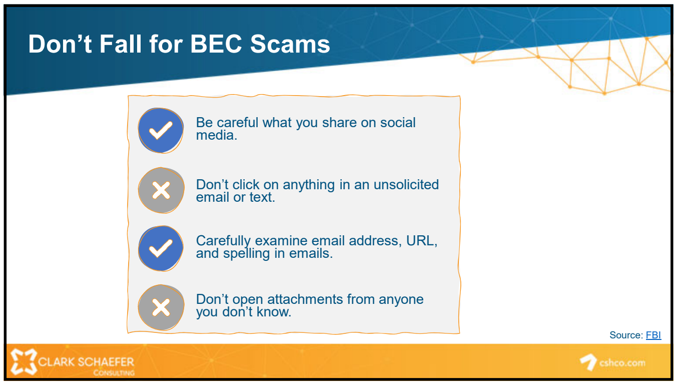
- **Send spearphishing emails**

  Looks like it's from a trusted sender

- **Use malware**

  Malicious software that can gain access to legitimate email threads

Source: FBI



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

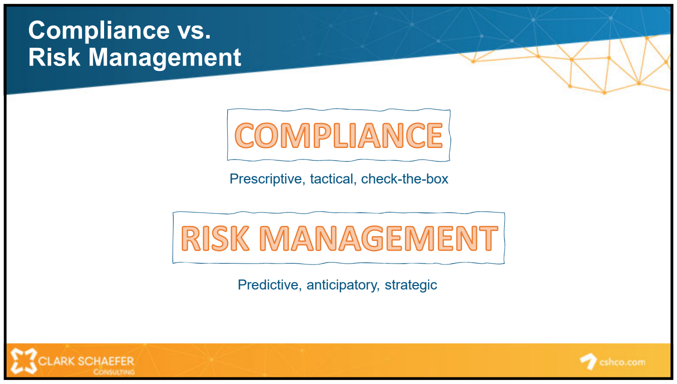
CLARK SCHAEFER CONSULTING

cshco.com

Managing Cybersecurity Risk

CLARK SCHAEFER CONSULTING

cshco.com



Compliance vs. Risk Management

COMPLIANCE

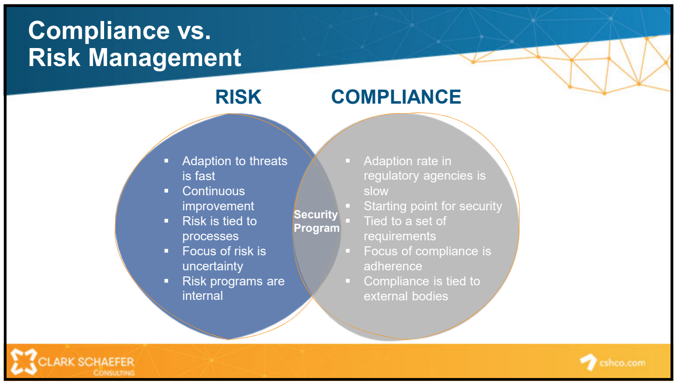
Prescriptive, tactical, check-the-box

RISK MANAGEMENT

Predictive, anticipatory, strategic

CLARK SCHAEFER CONSULTING

cshco.com



Compliance vs. Risk Management

RISK

- Adaption to threats is fast
- Continuous improvement
- Risk is tied to processes
- Focus of risk is uncertainty
- Risk programs are internal

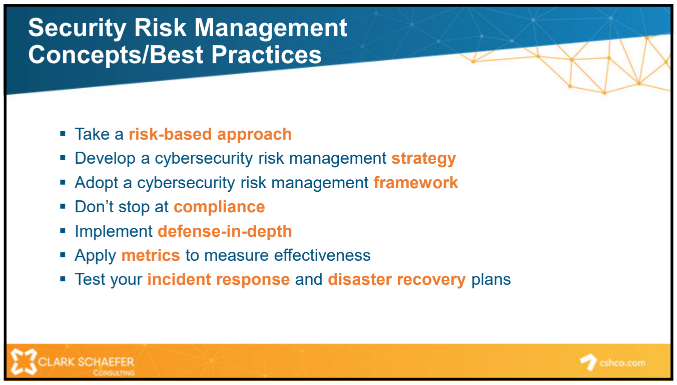
Security Program

COMPLIANCE

- Adaption rate in regulatory agencies is slow
- Starting point for security
- Tied to a set of requirements
- Focus of compliance is adherence
- Compliance is tied to external bodies

CLARK SCHAEFER CONSULTING

cshco.com

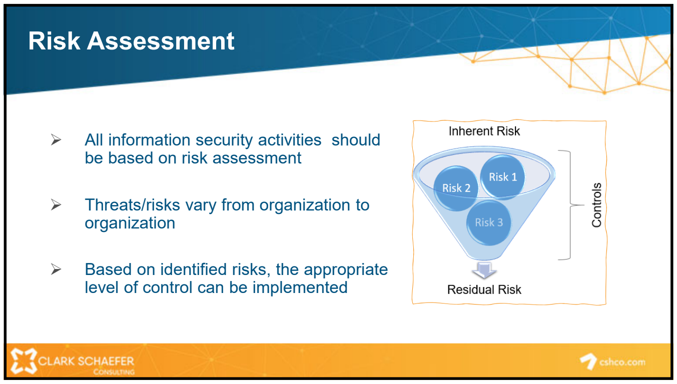


Security Risk Management Concepts/Best Practices

- 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

CLARK SCHAEFER CONSULTING

cshco.com



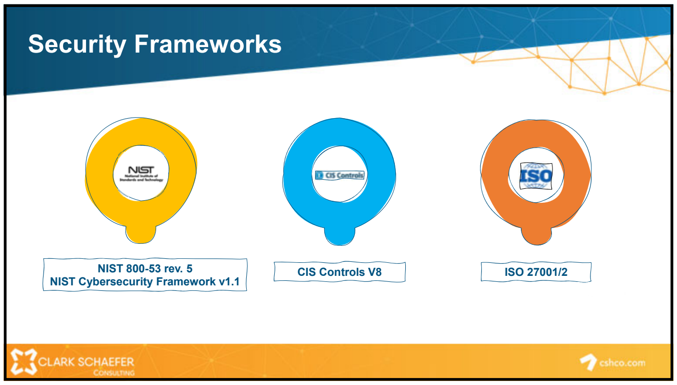
Risk Assessment

- 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

Inherent Risk
Risk 1
Risk 2
Risk 3
Controls
Residual Risk

CLARK SCHAEFER CONSULTING

cshco.com



Security Frameworks

NIST 800-53 rev. 5
NIST Cybersecurity Framework v1.1

CIS Controls V8

ISO 27001/2

CLARK SCHAEFER CONSULTING

cshco.com

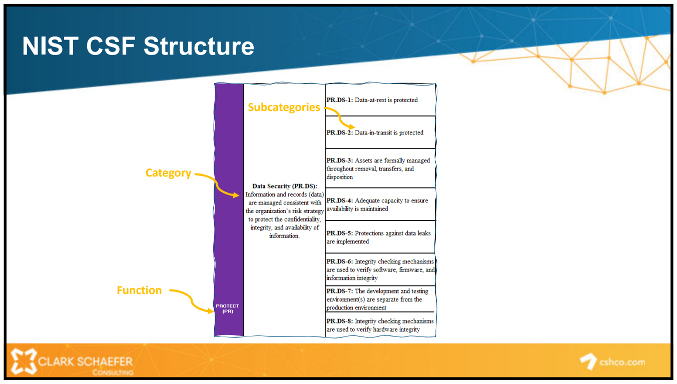
NIST CSF

- **5 Functions**
  Identify, Protect, Detect, Respond, Recover
- **23 Categories**
  Think of these as control objectives
- **108 Subcategories**
  Think of these as controls

RISK
MAXIMUM
HIGH
MEDIUM
LOW
MINIMUM

CLARK SCHAEFER CONSULTING

cshco.com



NIST CSF Structure

Subcategories

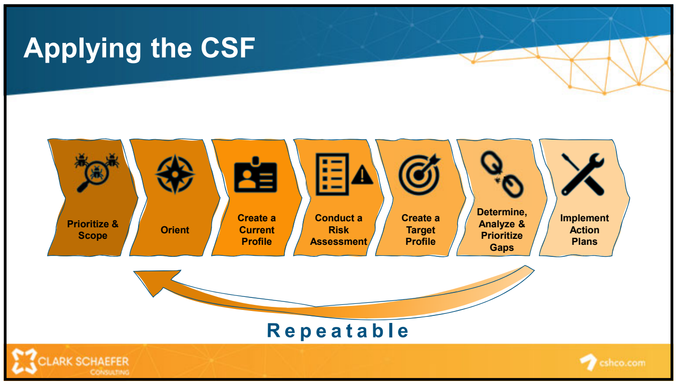
Category

Function

PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained
		PR.DS-5: Protections against data leaks are implemented
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7: The development and testing environment(s) are separate from the production environment
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity

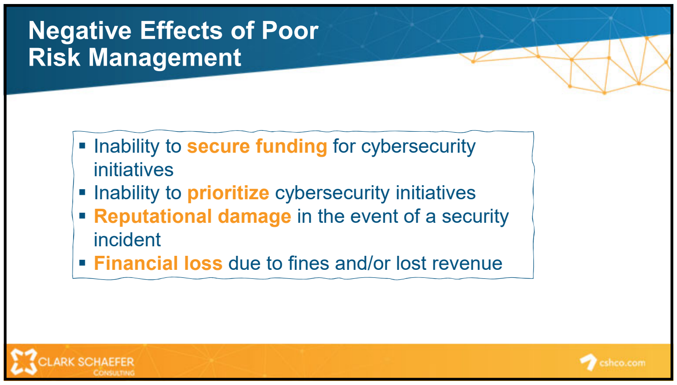
CLARK SCHAEFER CONSULTING

cshco.com



Applying the CSF

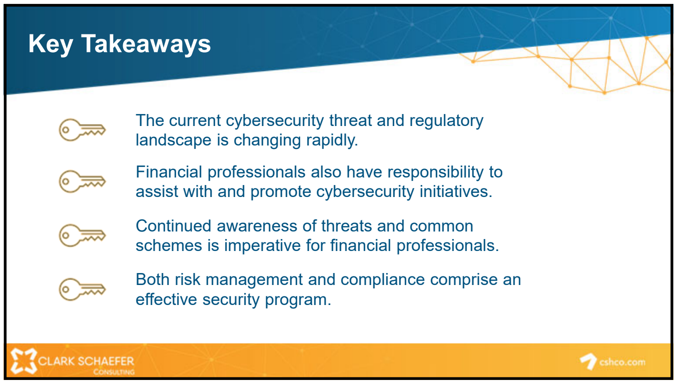
CLARK SCHAEFER CONSULTING cshco.com



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

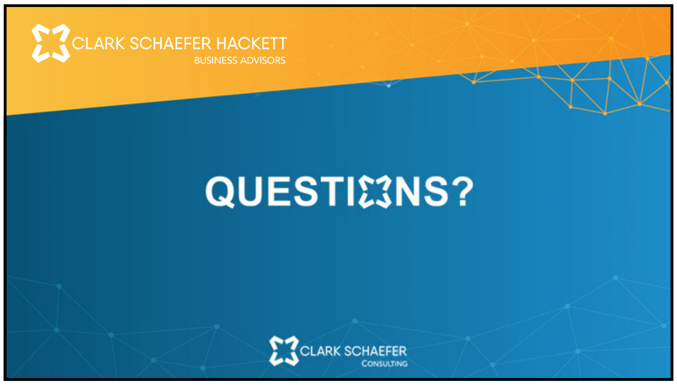
CLARK SCHAEFER CONSULTING cshco.com



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 CONSULTING cshco.com



CLARK SCHAEFER HACKETT
BUSINESS ADVISORS

QUESTIONS?

CLARK SCHAEFER
CONSULTING