

Cyber Security Awareness

What Agency Executives Need to Know

29-SEPTEMBER-2022

INFO-TECH RESEARCH GROUP

Mark A. Hoeting, Senior Executive Counselor

Agenda

01

Info-Tech – *A brief Introduction*

02

**Aspects of Effective Executive Communications on
Cyber Security**

03

Examples & Scenarios

About Info-Tech Research Group

A Step-By-Step Program to Systematically Improve Your IT & Security Organizations

Info-Tech Research Group is the world's fastest growing information technology research and advisory company, proudly serving over 30,000 IT professionals.

We produce unbiased and highly relevant research to help CIOs, CISOs, and IT leaders make strategic, timely, and well-informed decisions. We partner closely with IT teams to provide everything they need, from actionable tools to analyst guidance, ensuring they deliver measurable results for their organizations.

Communications to Agency Executives

Ground Rules for Engagement

1. Seek First to Understand
2. Understand Executive Perspectives
3. Prepare Relentlessly
4. Develop a Clear Agenda
5. Stick to Main Points
6. Maintain Consistency
7. Use a Framework
8. Focus on Agency Risks
9. Talk Agency Risks
10. Anticipate Questions

Seek First to Understand

Executives Have a Lot To Consider

01



Executives have major priorities focused on....

- What are the core services we provide?
- Aligning with strategy of elected officials.
- Achieving societal impact.
- Protecting assets and operations.

Understand Executive Perspectives

Perspective is Paramount

02



Get to Know Your Agency Executive, if Possible

- Most have a biography published online.
- Learn their background to gain insight into communications preferences.
- Develop a re-usable onboarding packet.
- Develop relationships with the inner circle.
- Protecting assets and operations.

Prepare Relentlessly

Executive Comms are High Stakes

03

Treat Agency Executive Communications as the High Stakes Game that it Is.

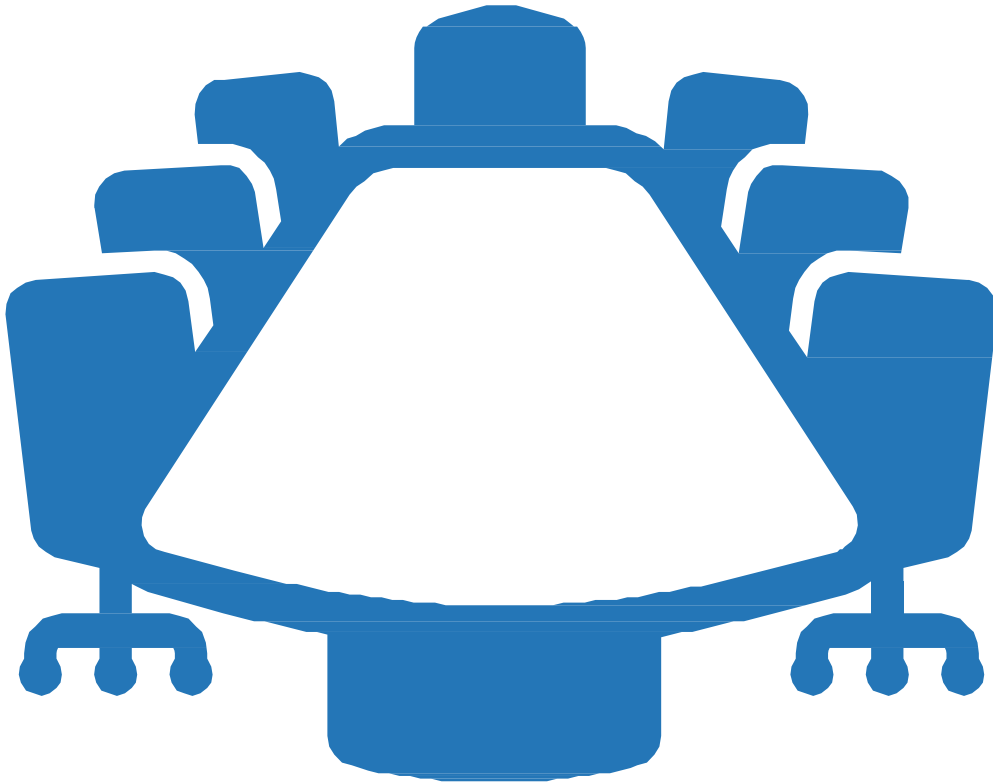
- Preparation should take days, not hours.
- Adequate preparation pays dividends, both for the CISO and the organization.
- Well-planned communications builds credibility with Agency Executives and Boards.
- Rehearse, edit, revise, rehearse.



Develop a Clear Agenda

Speak the Language of Business

04



Focus on the Executive Priorities

- Every interaction, both planned and unplanned should:
 - Focus on agency priorities
 - Do not reference the CISO/Org
- Leverage Data Points that are central to strategic priorities.
 - These are usually NOT data points from within IT or Cyber Security.

Main Points Only

How Are You Reducing Risk? How can they Help?

05



How much risk have you and your team reduced?

- Be Concise: How has the Cyber-security program reduced risk for the agency in the last period?
- Do not stray from main points aside from supporting data.
- Let data speak for itself, re-enforcing your point.

Maintain Consistency

Strengthen Your Message

06



Consistency in Message increases Executive Awareness of Cyber Priorities.

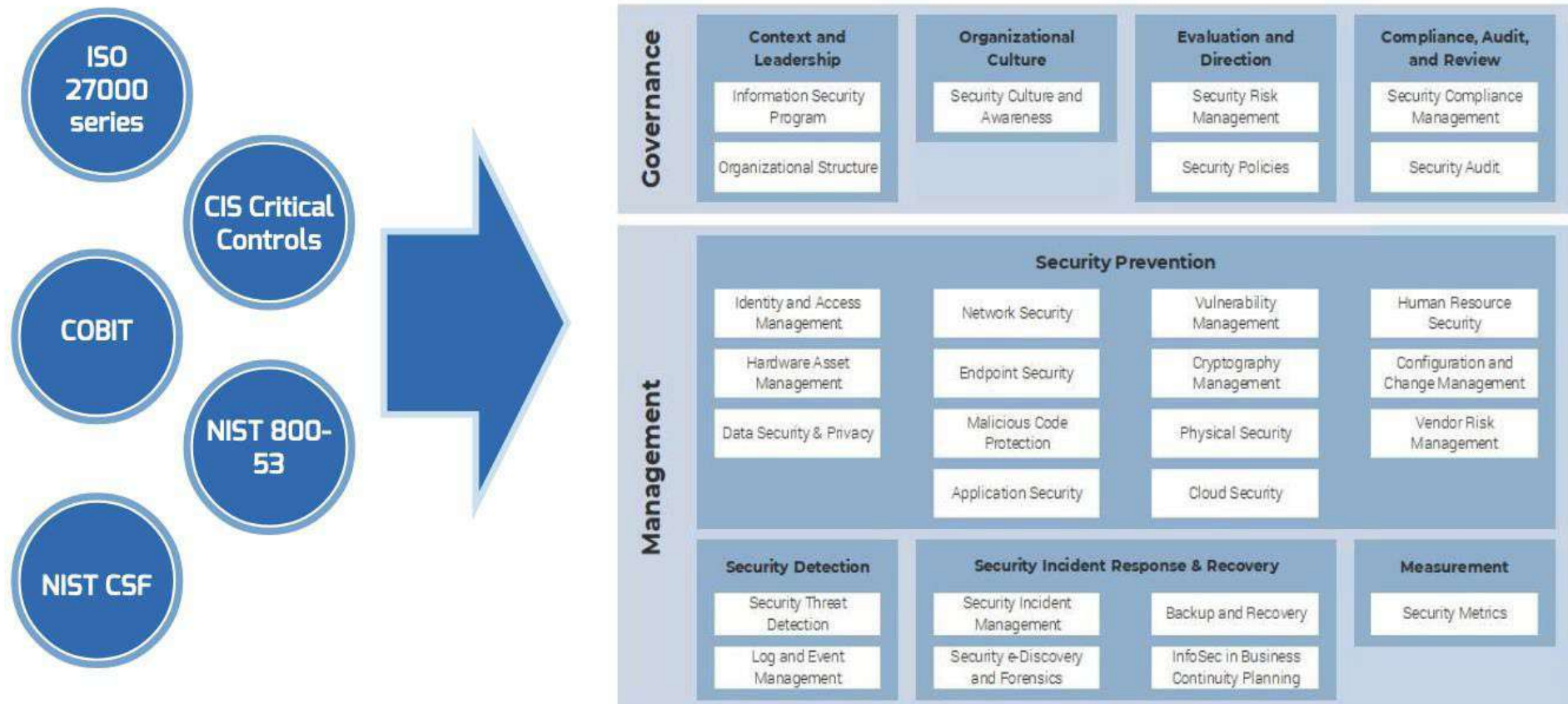
- Consistency in Message
- Consistency in Tone
- Consistency in Format

Use A Framework

Frameworks Reinforce Consistency

07

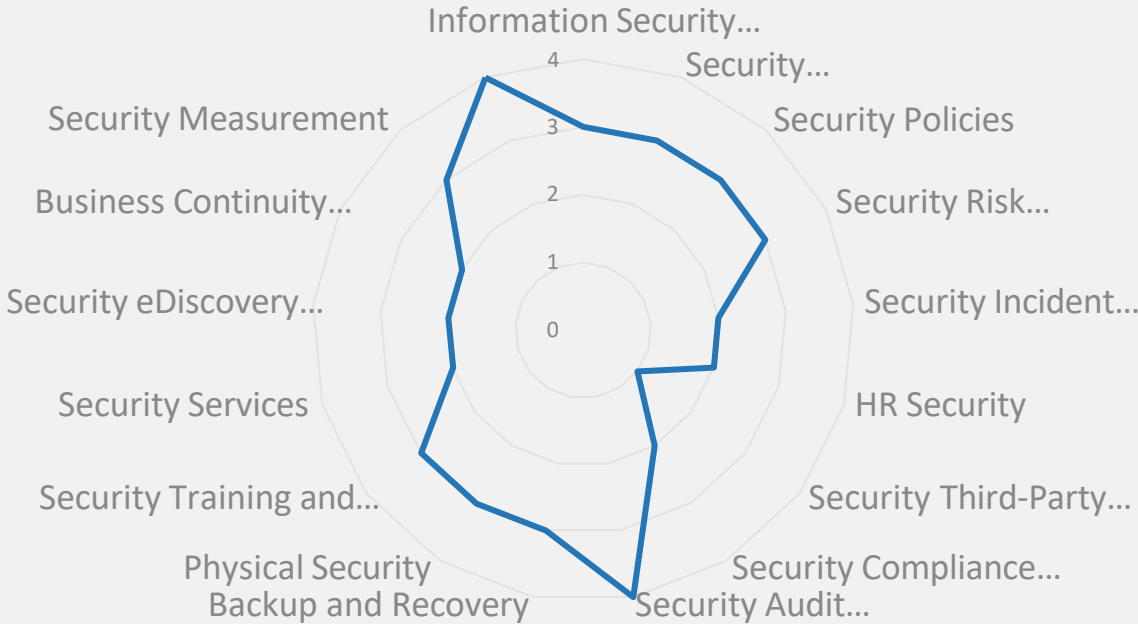
Info-Tech's framework integrates several best practices to create a best-of-breed security framework



Use A Framework

Frameworks are Data Driven

Security Governance Target Framework and Gap Analysis Tool						
Instructions Select your Security Pressure Posture (from the Security Pressure Posture Tool) from the drop box below. Use the recommended baseline as a starting point and customize your components in the Target State column if necessary. If no customizations are required, copy and paste the Recommended Baseline Targets into the Target State column. Document your current state in its respective column and the gap between your target state and current state. Summarize the actions required to fill the gap in the Gap Summary and scale the size of your gap in the Gap Scale column.						
Our Security Pressure Posture is		Low				
Components	Recommended Baseline Target	Target State	Current State	Gap Detail	Gap Summary	Gap Scale (1-5)
Information Security Charter	Security Vision, Security Mission, Security Objectives, Security Responsibilities, Organizational Responsibilities, and Governance Principles	E.g. Secu				
Security Organizational Structure	Security Reporting Structure, Management Commitment, RACI Chart	Security R				
Security Policies	Passwords Policy, Acceptable Usage Policy, Incident Response Policy, Risk Assessment Policy, Media Protection Policy, Personnel Security Policy	Passwords Policy, Inc Assessme Policy, Pe Manage Authentic Data Secu Policy, Aw Security A Infrastruct Control Po Contingen Configurati Policy, Sy Policy				
Security Risk Management	Risk Assessment Methodology, Risk Tolerance Level, Risk Management Process, Risk Tracking and Reporting	Risk Asse Tolerance Process, f				
Security Incident Management	Security incident identification, categorization and classification, incident response process and responsibilities, incident tracking and reporting, learning from security incident	Security in categoriza response i incident tr from secu process w				
HR Security		Prior to an and Termi Identify th				
Security Third-Party Management		Prepare to Manage th				
Security Compliance Management		Complianc Complianc security p				



Focus on Agency Risks

The Cyber Brand is Risk Mitigation

08



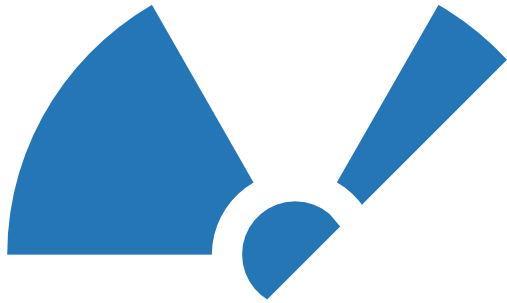
Your Organization's Brand should Always Reflect Something about Business Risk

- Understand your Organization's risk:
 - Industry Risks
 - Risks to Citizen Services
 - Risks to Revenue
- Sources to Consider
 - Peer Organizations
 - Audit Committees
 - Annual Audit Reports
 - Industry Resources & Trends

Talk Agency Risk

Risk is an Executive Language

09



Talk Agency Risks –
Not Fear & Tactics

Uncertainty has been over-utilized

Anticipate Questions

All Risk is Local...

10

These questions should be reviewed to position responses for most executive security questions:



- How do we compare to our peer agencies?
- How are we monitoring emerging threats and staying ahead of the curve?
- What are our breach detection & response capabilities?
- What are our greatest cyber security risks?
- Are we compliant with required cyber security regulations?
- How do we know if we have NOT been breached?
- How are we integrating cyber security risk into our enterprise risk-management program?
- Are we allocating enough resources for the cyber security program?

What Agency Executives Need to Know

Presenting to Executives



Summary Since Last Report

Business Risks

The Threat Environment

Program Trends

Security & Risk Update

This section focuses on presentation material on the security function of the organization. With the current landscape of security threats and incidents, these types of presentations are becoming increasingly popular and necessary to the board of directors.

This presentation includes:

- Security goals and objectives
- Key security metrics
- Recent security incidents and lessons to be learned from them
- Top threats and risks for the company and their business impacts
- Risk mitigation strategies and roadmap

Key Takeaways

01

Our security operations focus on three key goals; reduce the likelihood of data breaches, reduce business disruptions, and improve compliance.

02

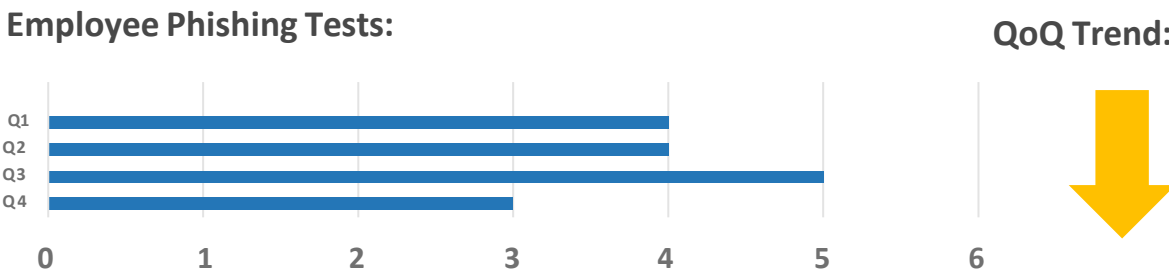
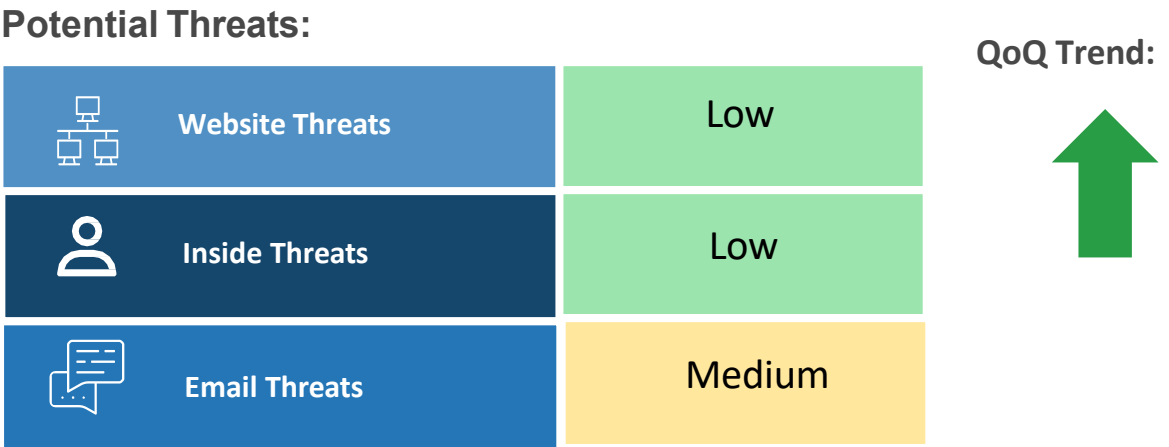
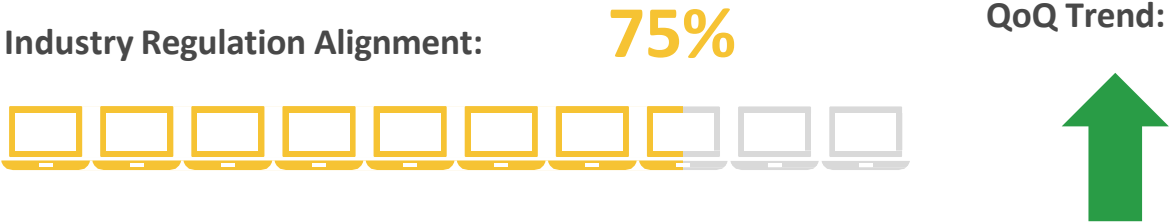
Our Security Risk Management program has identified two major risks to mitigate; major vulnerability on a legacy system, and confidential data that is not encrypted or protected.

Security Goals & Objectives

Meaningful, Practical, Compliant

Business Goals That Security Supports

- 1. Alignment with standard industry framework (e.g., ISO)
- 2. Reduction of security friction
- 3. Improved training and awareness
- 4. Reduction of costs associated with security incidents (e.g., data breach, regulatory fine)
- 5. Reduction of downtime associated with security incidents



Recent Security Lessons to be learned

Agency X



Highlight any recent security incidents or breaches that have impacted your industry or peers. It is important to show the board that IT is being proactive about security measures and protocols and learning from incidents outside the organization.

Incident: cyber attack, ransomware, data breach, etc.

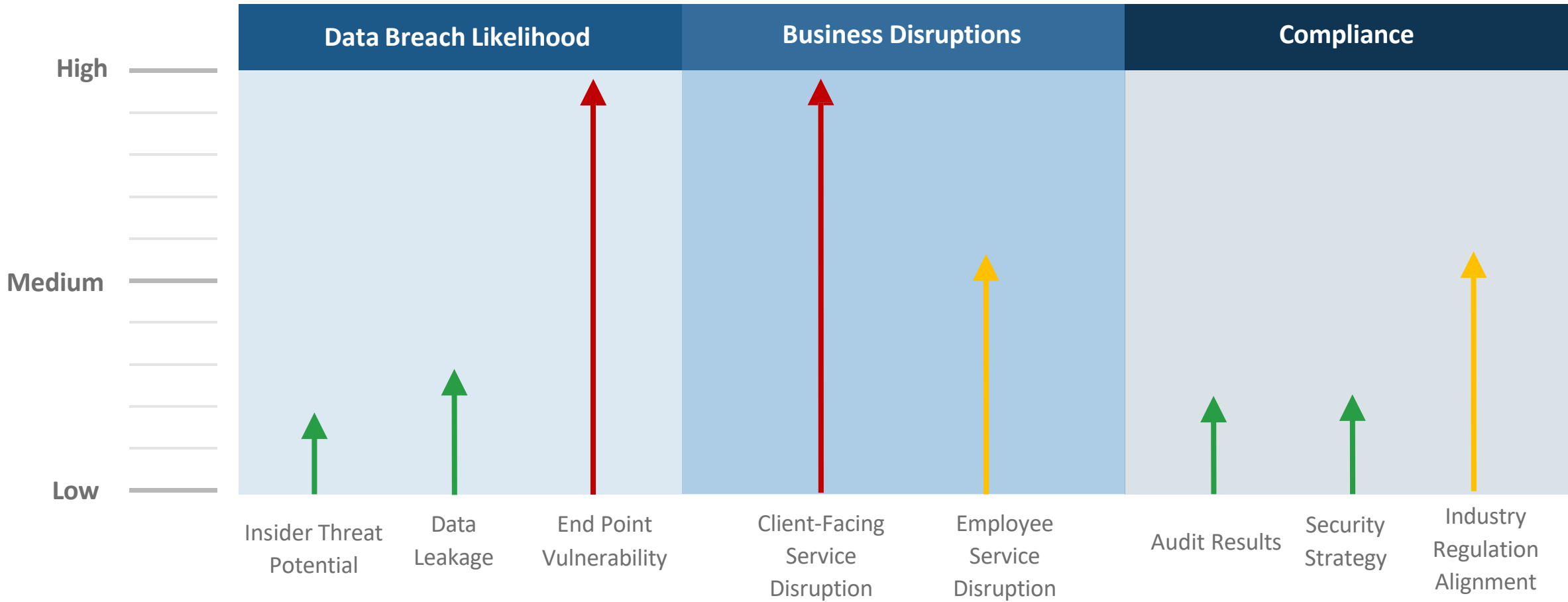
Response: how did the company respond and how were they prepared to minimize risks?

Lessons Learned: what can our company learn and adopt from this?

Top Threats & Risks

Assessing risk and threats to an organization is a huge effort. Communicate ITs preparedness in identifying and dealing with any threats that will impact the health of the business. Less emphasis on specific security protocols or technology solutions and a larger emphasis on business outcomes.





<Tagline> : Cyber threats are always evolving and there is no silver bullet. The team has adopted a proactive approach to risk identification and analysis.



*Refer to appendix for further information

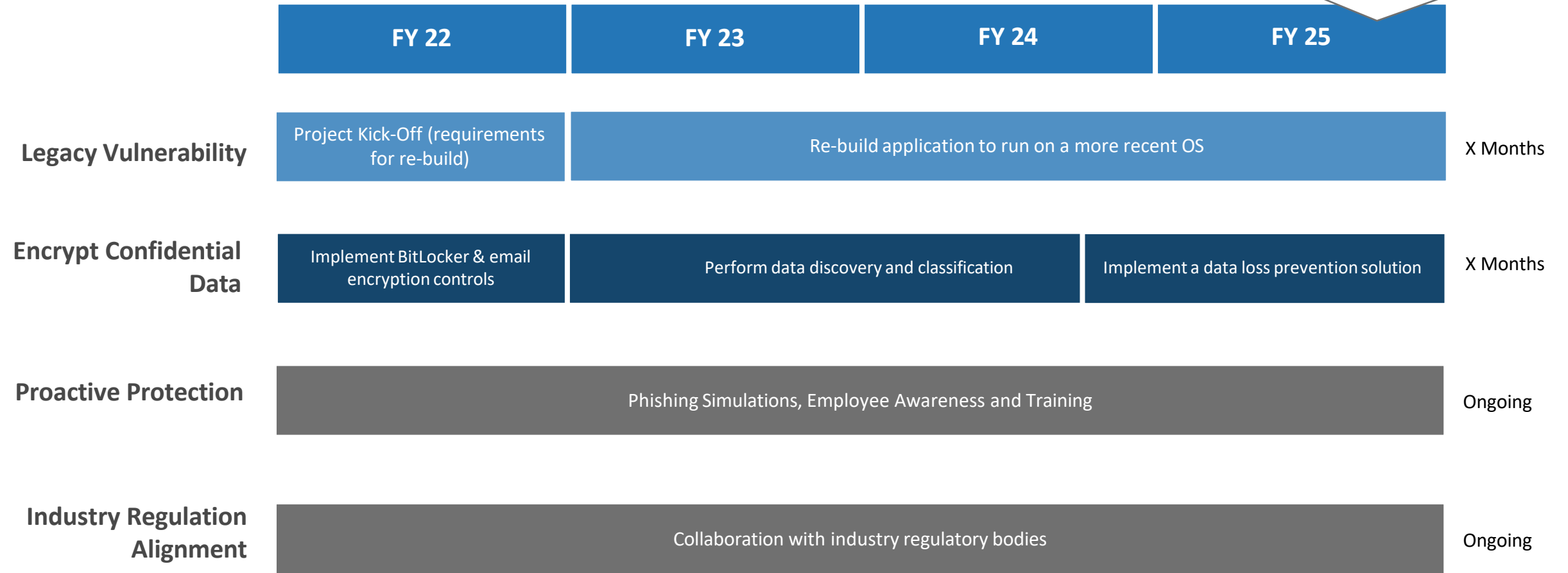
Risk Analysis

Clearly highlight the gaps and impacts of security threats to the board. Make a strong case for why these risks must be mitigated and ensure you have a strong rationale for your ask from board members.

	Risk	Business Impact	The Ask
 Major Vulnerability	Major vulnerability identified on legacy system	Disruption to operations in sales, engineering, and operations departments	Hire two development and two security resources – action required
 Potential Service Disruption	Confidential data is not encrypted properly or protected	Customer data breach, severe regulatory fines in event of breach, and reputational damage	Hire one development and two security resources – action required
 Employee Service Disruption	Improving – increasing internal phishing simulations	Lack of employee awareness could result in phishing attacks and leaked information	Continued investment in internal training – no action required
 Industry Regulation Alignment	75% and increasing	Incomplete alignment could expose us to regulatory fines and penalties	Continued efforts in regulatory alignment – no action required

Risk Mitigation Strategies & Roadmap

Visually represent how you plan to solve the problem with a roadmap. Focus on when and what will lead to an effective solution and ensure you are transforming technical language to information your board can easily consume. The level of technical detail to include will depend on your board's appetite and knowledge of IT, so carefully consider your audience when constructing this slide.



Summary & Takeaway

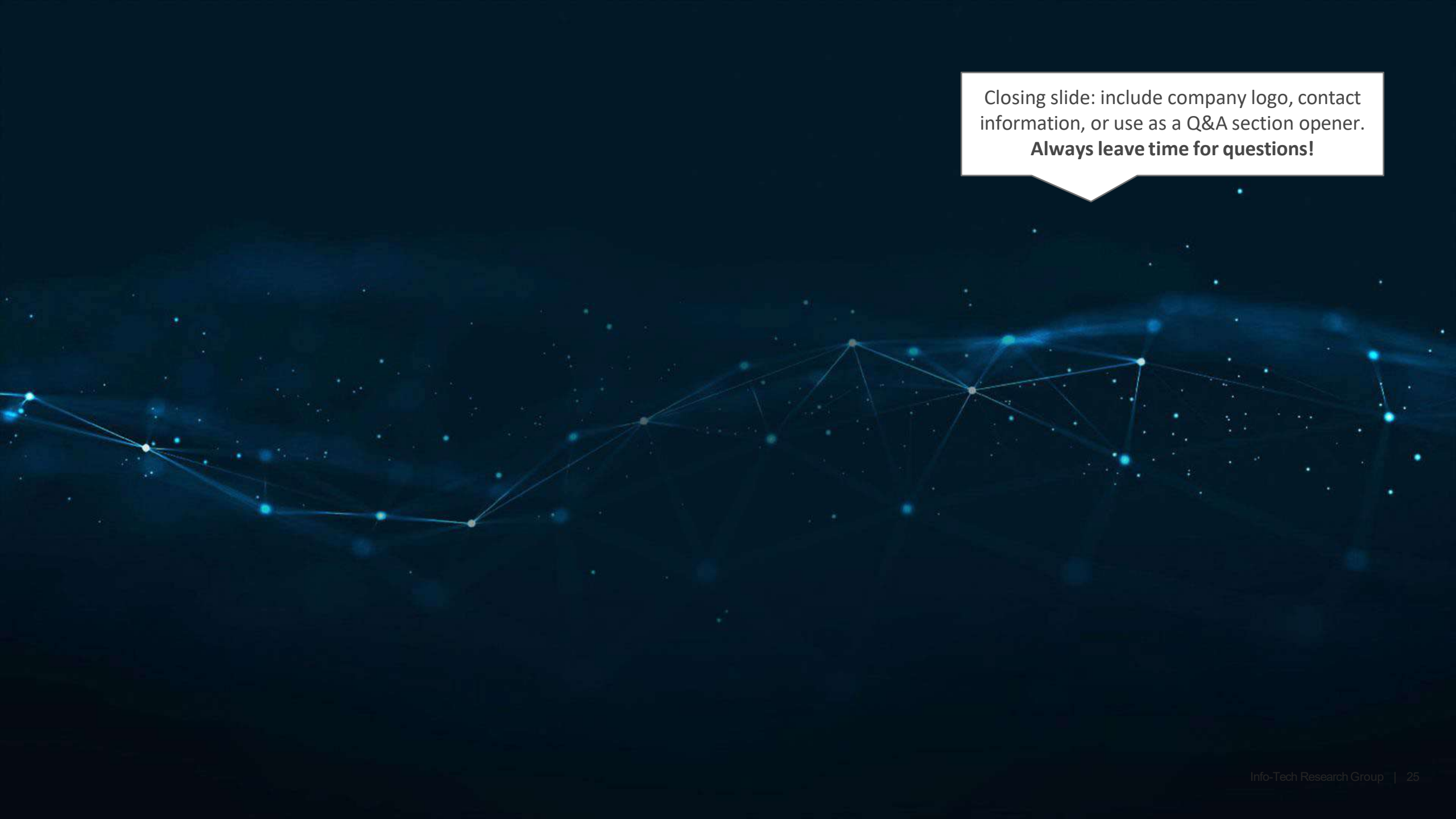
Wrap up your presentation with reminding the board of your key message and any action items outstanding for board members.

01

Cyber threats are always evolving, and our team is dedicated to employee training, regulation alignment, and proactive approaches to threat identification.

02

The board's sign-off on the proposed roadmap will ensure we are mitigating future threats effectively.



Closing slide: include company logo, contact information, or use as a Q&A section opener.

Always leave time for questions!

Appendix Slides: optional details on technology solutions. Leverage these slides to answer questions or dive deeper into the topic in your discussion with the board.

APPENDIX

Industry Framework or Maturity Model



Source: nist.gov



Source: imperva.com

Top Threats and Risks

Do NOT include dense and information-heavy slides in your presentation to the board. Include this information as pre- or post-presentation material or refer to it when answering questions.

<Tagline> : Cyber threats are always evolving and there is no silver bullet. The team has adopted a proactive approach to risk identification and analysis.

Risk 1: Data Breach Likelihood

Insider Threat Potential

- Low risk

Data Leakage

- Low risk

End Point Vulnerability

- Major vulnerability identified on legacy system

Risk 2: Business Disruptions

Client-Facing Service Disruption Potential

- Confidential data is not encrypted properly or protected

Employee Service Disruption Potential

- Improving – increasing internal phishing simulations

Risk 3: Compliance

Audit Results

- Strong

Security Strategy

- Completed & strong

Industry Regulation Alignment

- 75% and increasing

Security Risk Management Program

Do NOT include dense and information-heavy slides in your presentation to the board. Include this information as pre- or post-presentation material or refer to it when answering questions.



IDENTIFIED RISK

- Major vulnerability identified on sales application that runs on Windows XP.
- Windows XP is currently end of support, meaning that there will be no available patch.
- Application is used on a daily basis by the sales, engineering, and operations departments.



CURRENT MITIGATIONS

- Application is running on a virtual machine to avoid the potential for any lateral movement.
- Creation of non-admin accounts allows users to gain access to the system without having more access than needed.



RISK OPTIONS

- Action #1: Mitigate – Rebuild so that it can run on a more recent OS. This would require dedicated internal resources to focus on developing this or engaging an outside firm to do so.
- Action #2: Mitigate – Privileged access management (PAM) tools can be purchased to more effectively manage who accesses this application.
- Action #3: Terminate – The application can be terminated altogether (which can be done in conjunction with Action #1 to avoid operational loss).
- Action #4: Accept – Allow the application to continue running.

Risk #1
Major vulnerability identified on legacy

Risk Owner(s)
Sales, Engineering, Operations

Related Compliance Obligations
PCI

Cost	% spend in industry
Capex: \$\$	\$\$
Opex: \$\$	

Security Risk Management Program

Do NOT include dense and information-heavy slides in your presentation to the board. Include this information as pre- or post-presentation material or refer to it when answering questions.



IDENTIFIED RISK

- Confidential data is stored by the organization, including customer and employee personal data, but no active data controls are placed upon it.
- There are severe regulatory fines associated with the breach of personal data.



CURRENT MITIGATIONS

- The main mitigation is that employees are expected to know what to do with confidential data, but it should be noted that no formal training has taken place.



RISK OPTIONS

- Action #1: Mitigate – Implement BitLocker to ensure employees’ hard drives are encrypted. This will lead to a mean slower startup for devices, but it reduces risk from lost/stolen laptops data exfiltrated.
- Action #2: Mitigate – Implement email encryption controls. Employees will need to be trained on this and start using it regularly, which can cause friction.
- Action #3: Mitigate – Perform data discovery and classification. It will be necessary to understand what we consider critical for data and where it is located in the organization, but it can be an expensive and time-intensive initiative.
- Action #4: Mitigate – Implement a data loss prevention (DLP) solution to track how sensitive information can be exfiltrated. This can be expensive and will be reliant on formal classification being done in the first place.

Risk #2
Confidential data is not encrypted or protected

Risk Owner(s)
Legal, Finance, HR

Related Compliance Obligations
GDPR, HIPAA

Cost	% spend in industry
Capex: \$\$	\$\$
Opex: \$\$	

Company X's digital risk profile

This slide conveys an analysis of the different business risks. Board members will be very interested to learn about the scope of risks that the organization will be exposed to when introducing new and transformative ways to operate.

- High
- Medium
- Low



Digital transformation roadmap

Visually represent your transformation roadmap or the proposed timeline for your transformation initiatives.

01

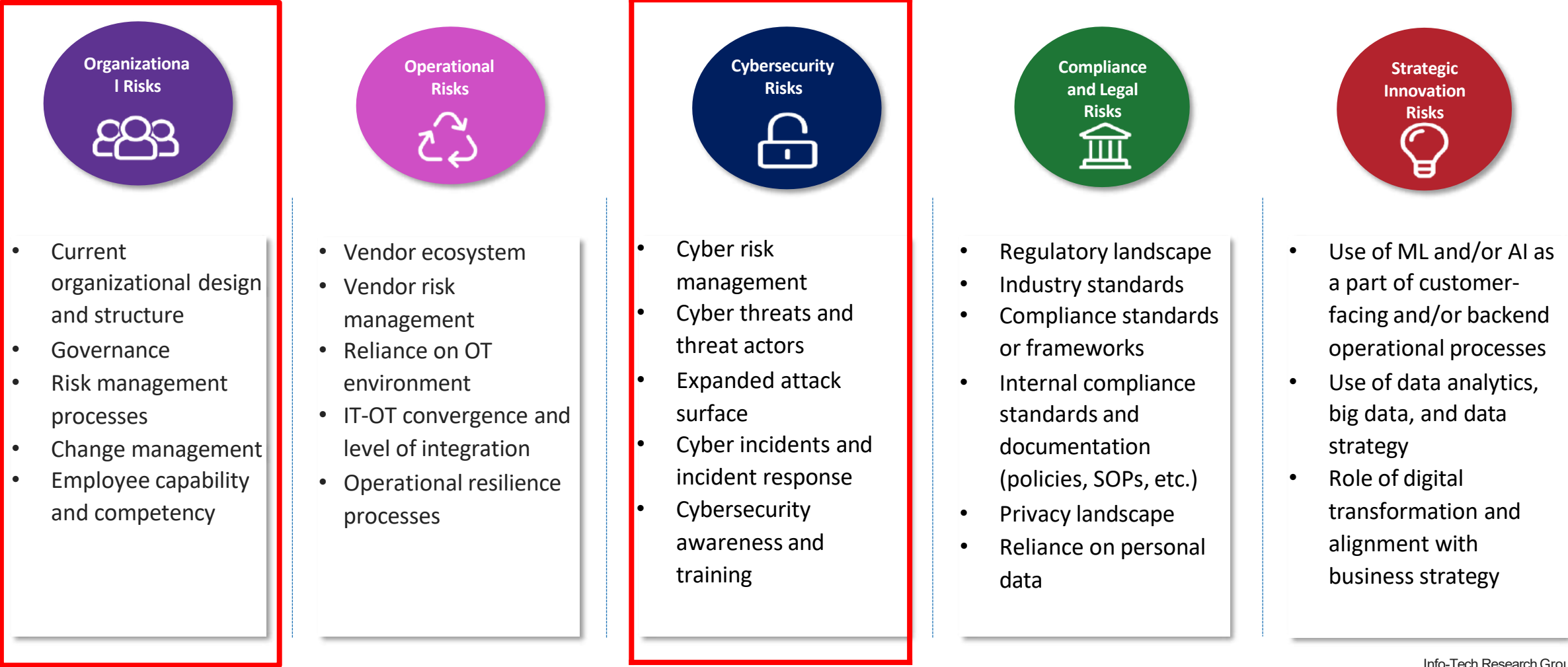
GOAL: Support hybrid course curricula development

Initiatives		
People		Initiative owner
1	Train researchers on functionality of centralized repository	Brittany
2	Define business value and assess user needs of tools	Anne
3	Provide training on tool types and align to user needs	John
Process		
4	Periodically review and validate data entries into central repository	Harry
5	Catalog software applications and tools across the organization	Christine
6	Identify under-used or duplicate tools/applications	Sharon
Technology		
7	Acquire and implement knowledge management application	Bob
8	Retire duplicate or under-used tools	Brittany

#	Year 1				Year 2			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1								
2								
3								
4								
5								
6								
7								
8								

Profile of *[Agency Name]*'s digital risk

After completing the *Digital Risk Profile* tool, *[Agency Name]* has developed a clear picture of its core areas of exposure when it comes to digital risk categories.



[Agency X]'s digital risk profile

Risk Category	Subcategory	Adjusted Weighting		Risk	Category Risk
Organizational	Organizational Structure	50%	10%	High	High
	Change Management	30%		Low	
	Staff Awareness, Skills, & Training	20%		High	
Operational	Third-Party Management	30%	40%	Moderate	Moderate
	Third-Party Risk	25%		Moderate	
	Operational Process & Resilience	25%		Low	
	Operating Technology Environment	20%		Moderate	
Cybersecurity & IT	Cyber Risk	50%	30%	Very High	Very High
	Incidents	40%		Very High	
	Governance & Strategic Operations	10%		High	
Legal & Compliance	External Regulatory & Compliance Environment	20%	10%	Low	Moderate
	Internal Compliance Environment	50%		Moderate	
	Data Privacy	30%		High	
Strategic Innovation	Governance	40%	10%	Moderate	Low
	Operations	60%		Low	

THANK YOU

Cyber Security Awareness
What Agency Executives Need to Know

29-SEPTEMBER-2022

INFO-TECH RESEARCH GROUP

Mark A. Hoeting, Senior Executive Counselor

Info-Tech Research Group Inc. is a global leader in providing IT research and advice.
Info-Tech's products and services combine actionable insight and relevant advice with
ready-to-use tools and templates that cover the full spectrum of IT concerns.
© 1997-2020 Info-Tech Research Group Inc.

INFO~TECH
RESEARCH GROUP

Your Info-Tech Team



Mark Hoeting

Senior Executive Counselor

mhoeting@infotech.com



Chris Dunn

Member Services Director

chris.dunn@infotech.com

About Us

To receive Security Briefing Deck:



Info-Tech Research Group is the world's fastest growing information technology research and advisory company, proudly serving over 30,000 IT professionals.

We are, by far, the most innovative firm in the industry and we pride ourselves on providing better research than anyone.

Since 1997, we have been helping CIOs, CISOs, and their teams evolve from firefighters to innovation champions.

We produce unbiased and highly relevant research & tools to help IT leaders make strategic, timely, and well-informed decisions that drive business value.

We partner closely with IT teams to provide everything they need – from actionable tools to in-person analyst guidance—to deliver measurable results for their organizations.