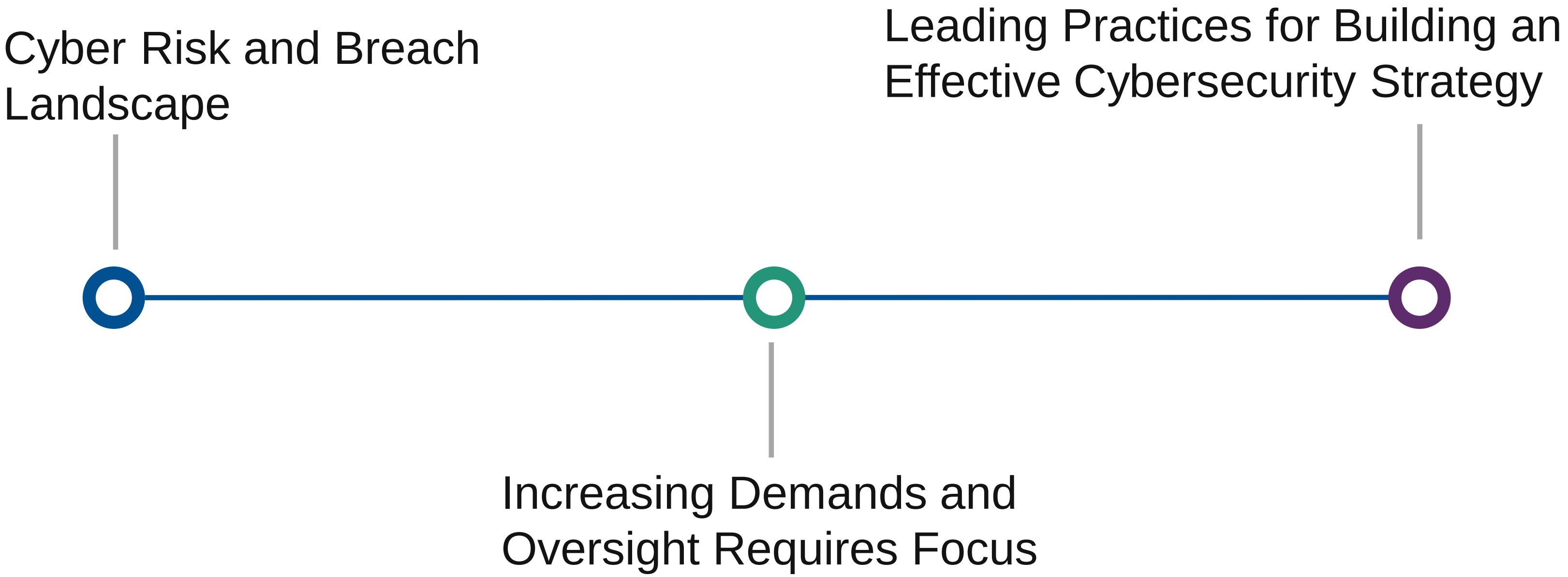
Building an Effective Cyber Security Strategy

Office of the CISO

Agenda



Cyber Risk and Breach Landscape

Increasing Demands and Oversight Requires Focus

Leading Practices for Building an Effective Cybersecurity Strategy

Top 25 Passwords

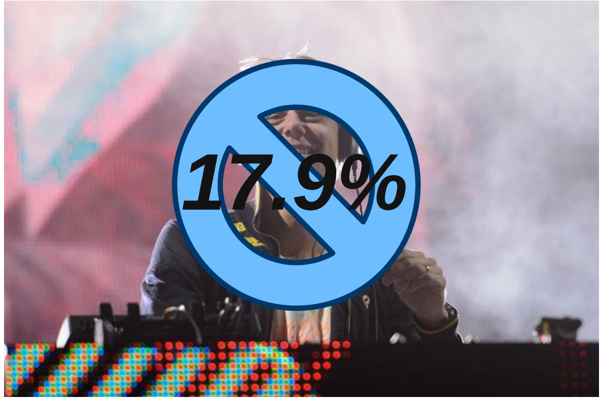
01. 123456 (Same)
02. password (Same)
03. 12345678 (Up 1)
04. qwerty (Up 1)
05. 12345 (Down 2)

06. 123456789 (Same)
07. football (Up 3)
08. 1234 (Down 1)
09. 1234567 (Up 2)
10. baseball (Down 2)

11. welcome (New)
12. 1234567890 (New)
13. abc123 (Up 1)
14. 111111 (Up 1)
15. 1qaz2wsx (New)

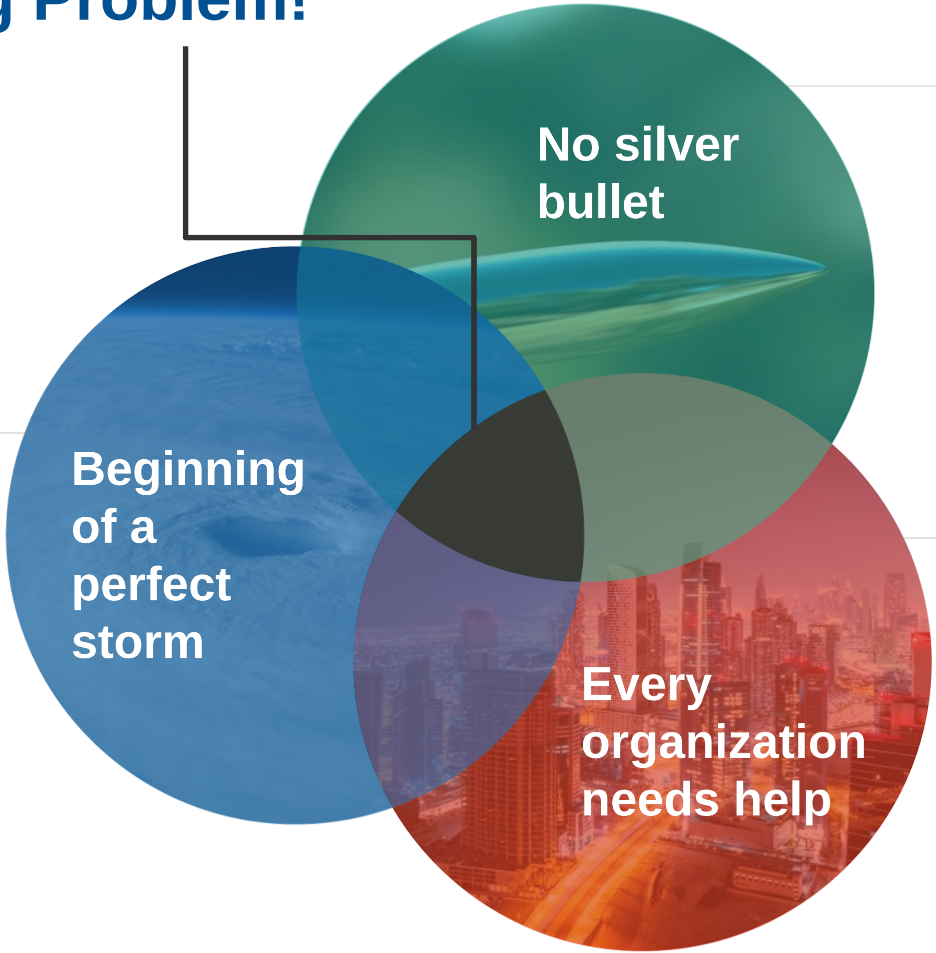
16. dragon (Down 7)
17. master (Up 2)
18. monkey (Down 6)
19. letmein (Down 6)
20. login (New)

21. princess (New)
22. qwertyuiop (New)
23. solo (New)
24. passw0rd (New)
25. starwars (New)



http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514?utm_campaign=socialflow_lifehacker_facebook&utm_source=lifehacker_facebook&utm_medium=socialflow

A Very Big Problem!



Nearly every tactic can be defeated

There is no one-size-fits-all solution

It will never be done

World wants to be more connected

Massive explosion/churn of infrastructure and data

Threat volume and sophistication growing exponentially every day

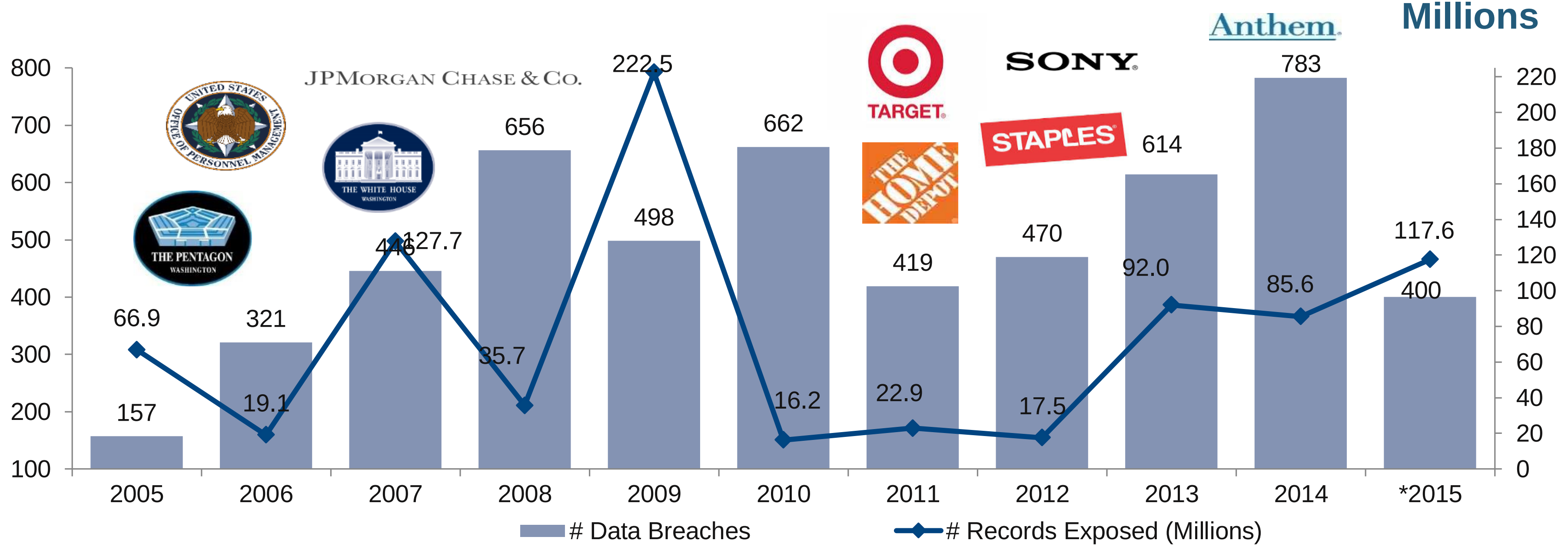
Stakes are high and getting higher

Thousands of options and choices

Few have the know-how, awareness, resources or time to catch up or keep up

Data Breaches and Records Exposed

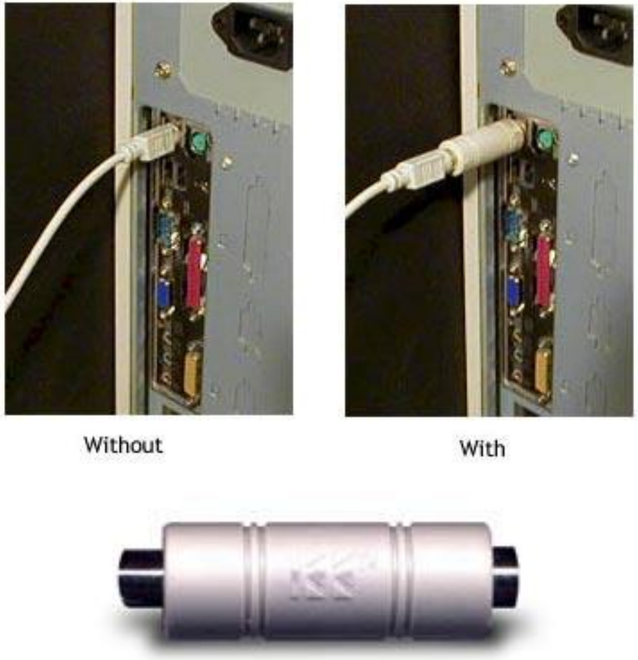
# Data Breaches/Millions of Records Exposed



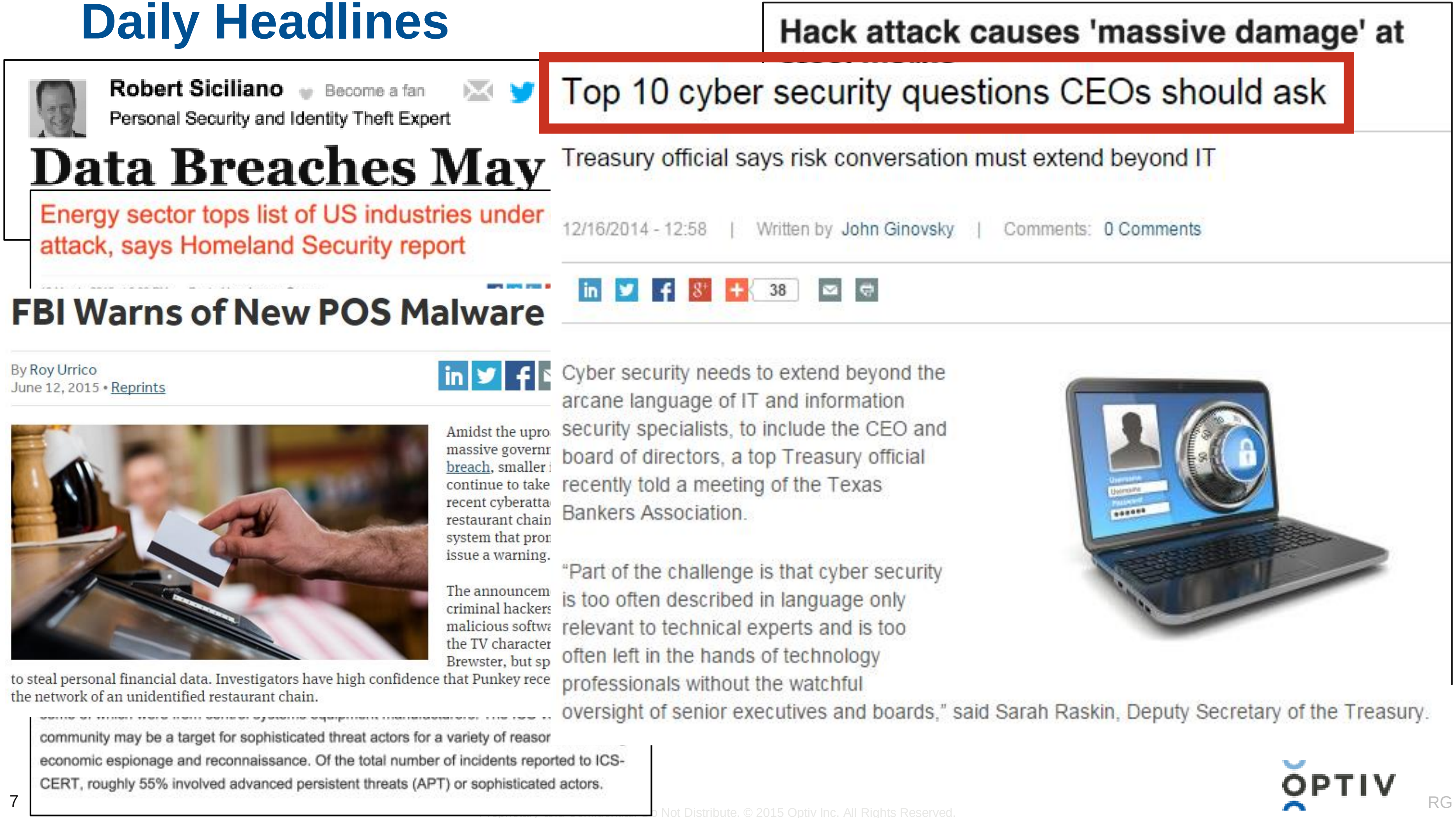
The total number of data breaches (+27.5%) hit a record high of 783 in 2014, exposing 85.6 million records. Through June 30, 2015 has seen 117.6 million records exposed in 400 breaches.*

*Figures as of June 30, 2015, from the Identity Theft Resource Center, http://www.idtheftcenter.org/images/breach/ITRCBreachReport2015.pdf

Stolen Records Are Only One Concern



Daily Headlines



Hack attack causes 'massive damage' at

Robert Siciliano Become a fan

Personal Security and Identity Theft Expert

Data Breaches May

Energy sector tops list of US industries under attack, says Homeland Security report

FBI Warns of New POS Malware

By Roy Urrico
June 12, 2015 • Reprints

Amidst the upro
massive governr
breach, smaller i
continue to take
recent cyberatta
restaurant chain
system that pror
issue a warning.

The announcem
criminal hackers
malicious softwa
the TV character
Brewster, but sp
to steal personal financial data. Investigators have high confidence that Punkey rece
the network of an unidentified restaurant chain.

community may be a target for sophisticated threat actors for a variety of reasor
economic espionage and reconnaissance. Of the total number of incidents reported to ICS-CERT, roughly 55% involved advanced persistent threats (APT) or sophisticated actors.

Top 10 cyber security questions CEOs should ask

Treasury official says risk conversation must extend beyond IT

12/16/2014 - 12:58 | Written by John Ginovsky | Comments: 0 Comments

38

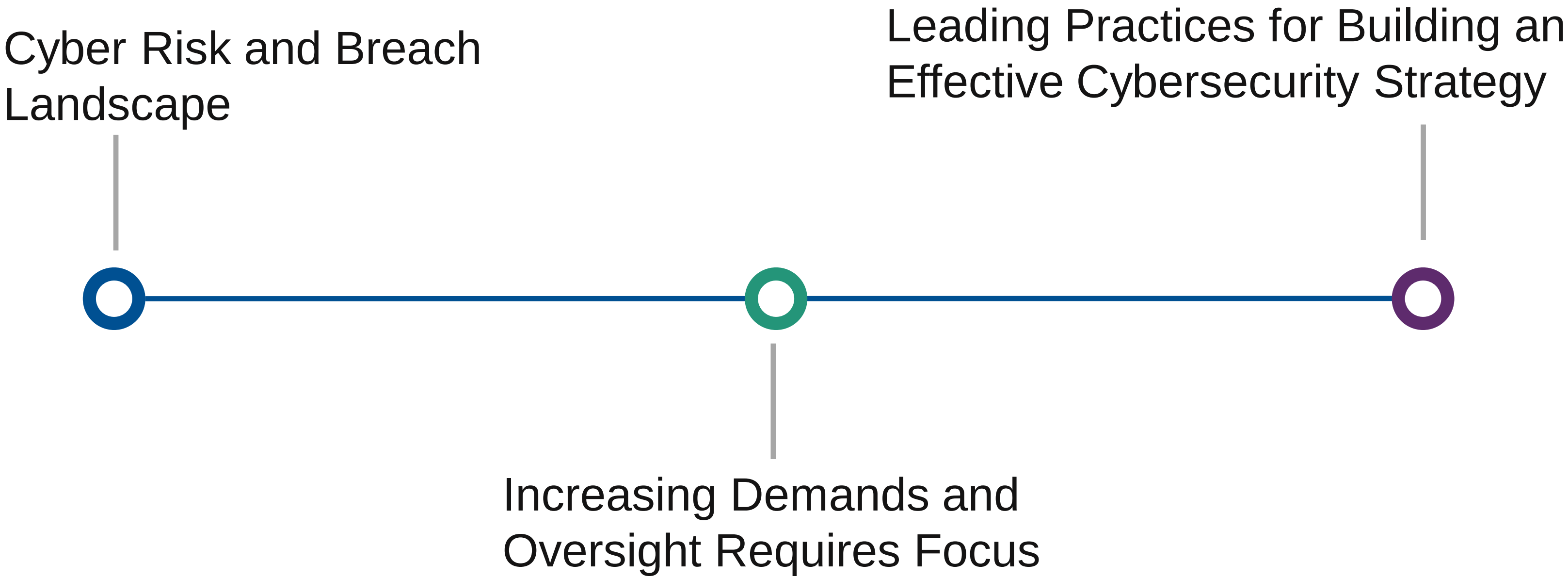
Cyber security needs to extend beyond the arcane language of IT and information security specialists, to include the CEO and board of directors, a top Treasury official recently told a meeting of the Texas Bankers Association.

"Part of the challenge is that cyber security is too often described in language only relevant to technical experts and is too often left in the hands of technology professionals without the watchful oversight of senior executives and boards," said Sarah Raskin, Deputy Secretary of the Treasury.

OPTIV

RG

Agenda



Cyber Risk and Breach Landscape

Increasing Demands and Oversight Requires Focus

Leading Practices for Building an Effective Cybersecurity Strategy

Five NACD Principles

Cyber-Risk Oversight

Executive Summary

DIRECTOR'S HANDBOOK SERIES

2014

1 Directors need to understand and approach cyber security as an **enterprise-wide risk management issue**, not just an IT issue.

2 Directors should understand **the legal implications** of cyber risks as they relate to their company's specific circumstances.

3 Boards should have adequate access to cyber security expertise, and **discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.**

4 Directors should set an **expectation that management establish an enterprise-wide cyber-risk management framework** with adequate staffing and budget.

5 Board-management discussions about cyber risk should include identification of which risks to avoid, accept, mitigate or transfer through insurance, **as well as specific plans associated with each approach.**

Sample NACD Questions

Questions Directors Can Ask to Assess the Board's "Cyber Literacy"

#2 Do we think there is adequate protection in place if someone wanted to get at or damage our corporate "crown jewels"? What would it take to feel comfortable that those assets were protected?

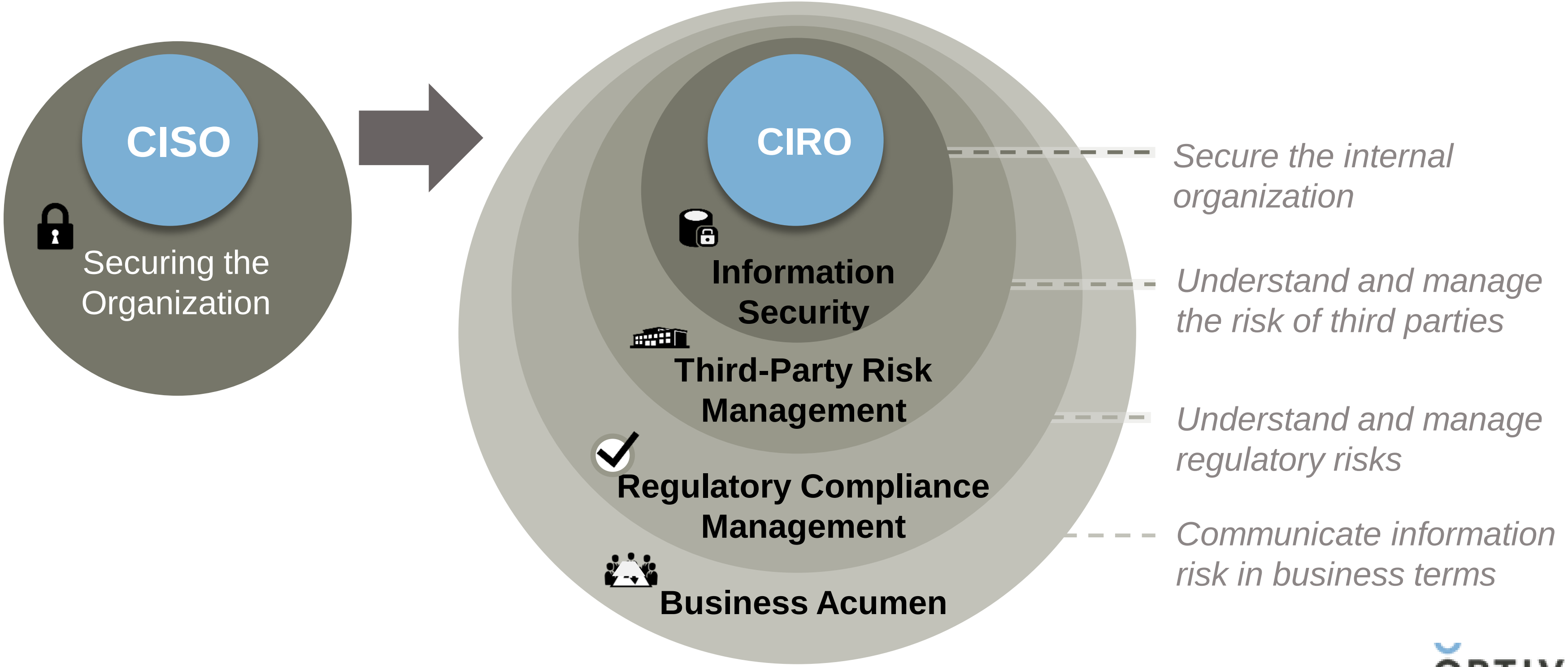
1. What do we consider our most valuable assets? How does our IT system interact with those assets? Do we believe we can ever fully protect those assets?
2. Do we think there is adequate protection in place if someone wanted to get at or damage our corporate "crown jewels"? What would it take to feel comfortable that those assets were protected?
3. Are we investing enough so that our corporate operating and network systems are not easy targets by a determined hacker?[1]
4. Are we considering the cybersecurity aspects of our major business decisions, such as mergers and acquisitions, partnerships, new product launches, etc., in a timely fashion?
5. Who is in charge? Do we have the right talent and clear lines of accountability/responsibility for cybersecurity?[2]
6. Does our organization participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organizations?
7. Is the organization adequately monitoring current and potential future cybersecurity-related legislation and regulation?[3]
8. Does the company have insurance that covers cyber events, and what exactly is covered?[4]
9. Is there directors and officers exposure if we don't carry adequate insurance?[5]
10. What are the benefits beyond risk transfer of carrying cyber insurance?[6]

From the National Association of Corporate Director's Cyber-Risk Oversight Director's Handbook Series 2014 Edition, page 17: http://www.aig.com/Chartis/internet/US/en/Financial%20Lines_Cybersecurity_Handbook_Global_tcm3171-639223.pdf.

OPTIV

Evolution of the CISO

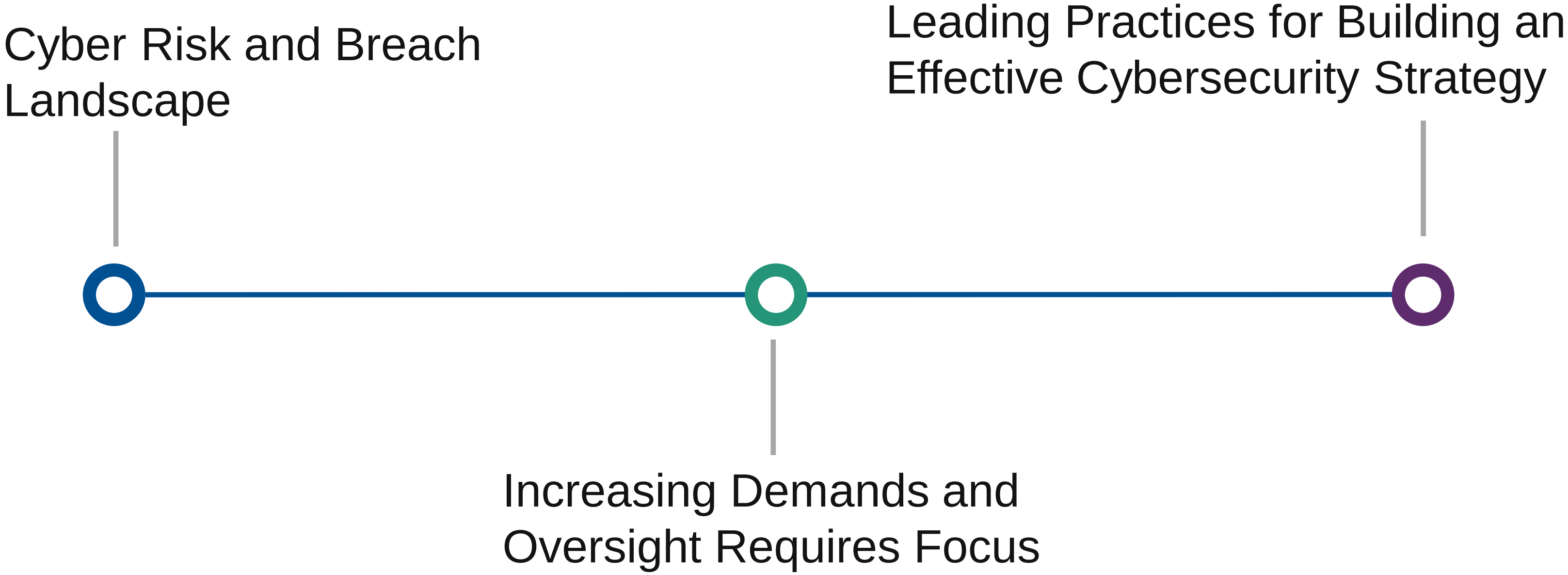
The focus has changed from protecting the IT infrastructure to managing the information risk to the organization


CISO
Securing the Organization
CIRO
Information Security
Third-Party Risk Management
Regulatory Compliance Management
Business Acumen
Secure the internal organization
Understand and manage the risk of third parties
Understand and manage regulatory risks
Communicate information risk in business terms

Problem Space Expands

Key
Hacking
Standards
Effective
Framework
Defending
Know
Model
Integrated
Implementing
Defense
Application
Success
Continuous
Mitigating
Sharing
Fraud
Real
Program
Certificate
Monitoring
Vulnerability
Critical
Awareness
Incident
Business
Approach
Service
Challenges
Network
Intelligence
Analysis
Solutions
Privacy
Detection
Professionals
Hackers
Making
Government
Internet
Architecture
Environments
Breach
Encryption
Case
Devices
Attacks
Strategy
Enterprise
Malware
PCI
Future
Analytics
Prevention
Virtual
Users
Automated
Control
Best
State
Improving
Management
Cloud
Threats
Software
Time
Web
Infrastructure
Using
Getting
DDoS
Legal
CISO
Work
Private
Study
Protection
Mobile
Information
Building
Evolution
Learned
Apps
APT
Chain
Assessment
Communication
Public
Policy
Operations
Insider
Product
Response
Cost
Code
Based
Access
Password
Global
Advanced
Lessons
Compromise
Risk
Cyber
Data
New
BYOD
Development
Authentication
Systems
Metrics
Exploit
Social
Trust
Compliance
Big
Testing
Industry
Identity
Practices
World
Techniques
Technology
Cybersecurity

Agenda

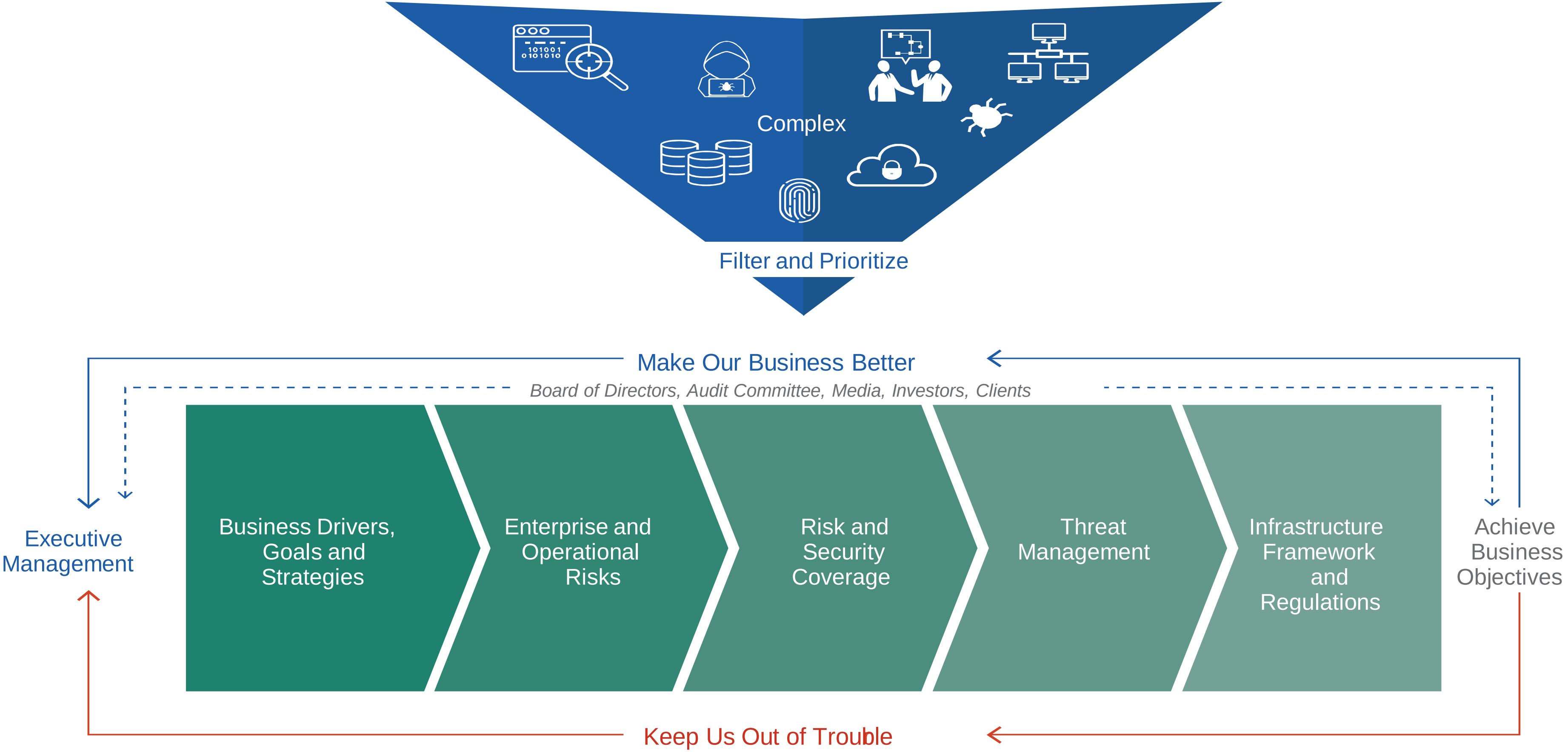


Cyber Risk and Breach Landscape

Increasing Demands and Oversight Requires Focus

Leading Practices for Building an Effective Cybersecurity Strategy

Business Aligned – Threat Aware Security Program



Complex

Filter and Prioritize

Make Our Business Better

Board of Directors, Audit Committee, Media, Investors, Clients

Executive Management

Business Drivers, Goals and Strategies

Enterprise and Operational Risks

Risk and Security Coverage

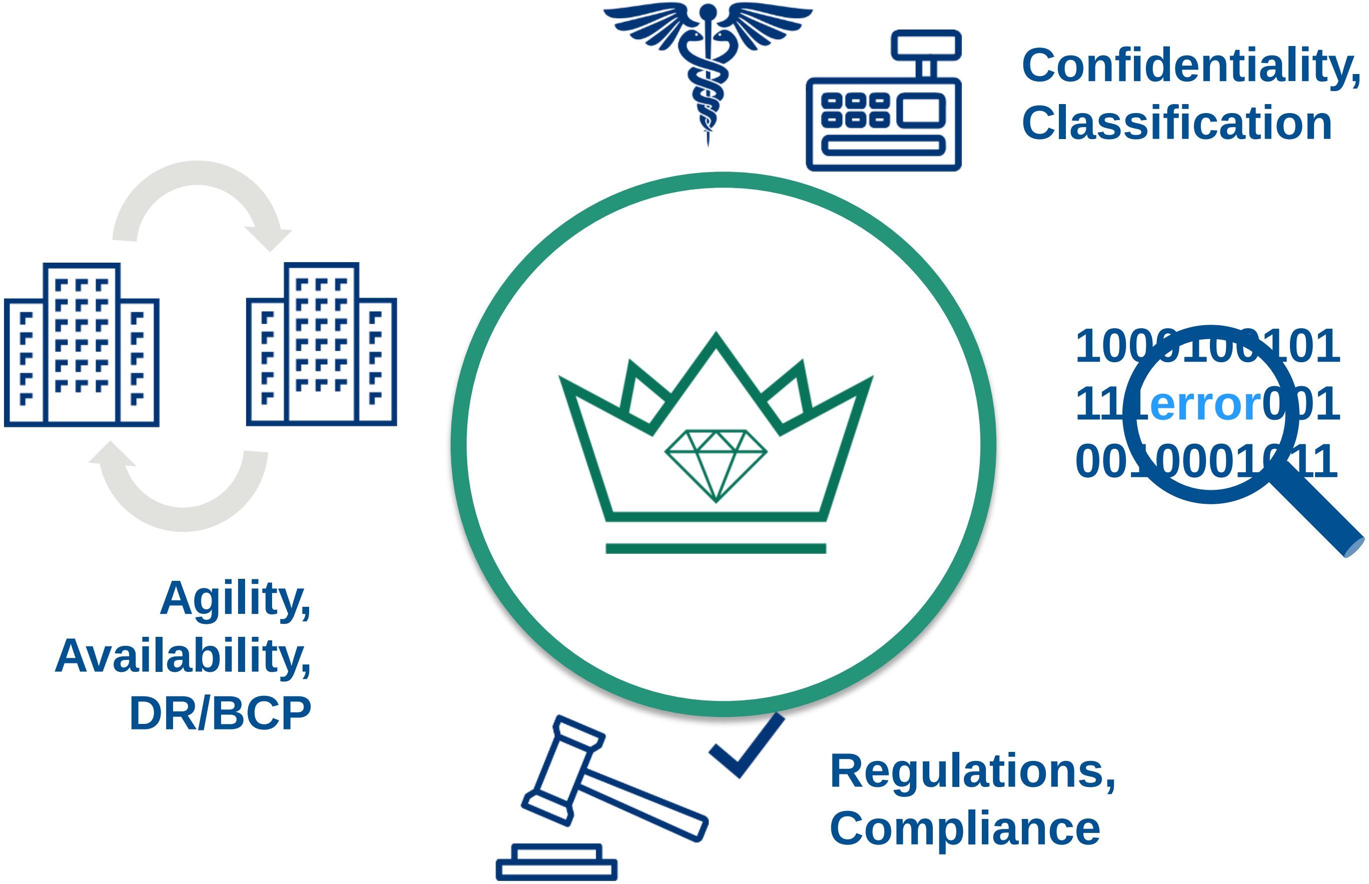
Threat Management

Infrastructure Framework and Regulations

Achieve Business Objectives

Keep Us Out of Trouble

Focus on Business Critical Systems and Data



Confidentiality, Classification

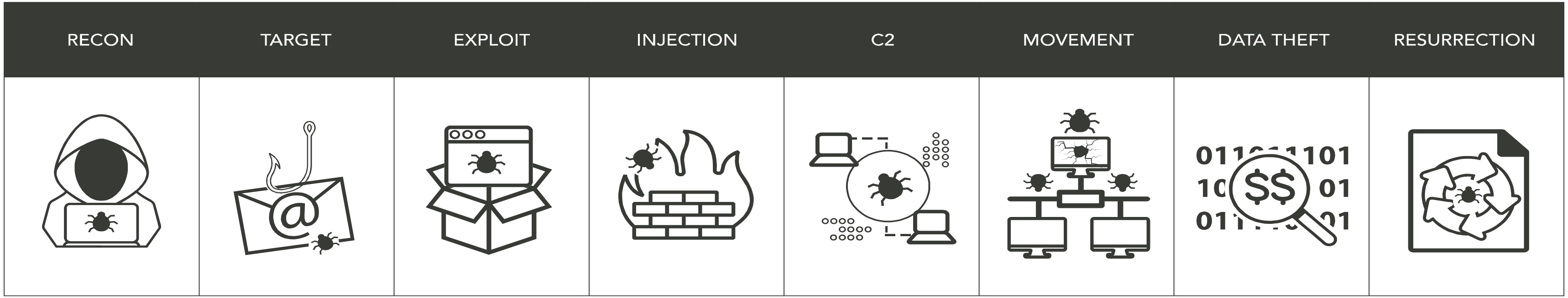
Integrity, Validity

Regulations, Compliance

Agility, Availability, DR/BCP

Understand Threats Across Entire Attack Lifecycle

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Network Attack
Objective	Access & Propagation	Economic, Political Advantage	Financial Gain	Defamation, Press & Policy	Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat	Credit Card Theft	Website Defacements	Destroy Critical Infrastructure
Character	Automated	Persistent	Opportunistic	Conspicuous	Conflict Driven



RECON

TARGET

EXPLOIT

INJECTION

C2

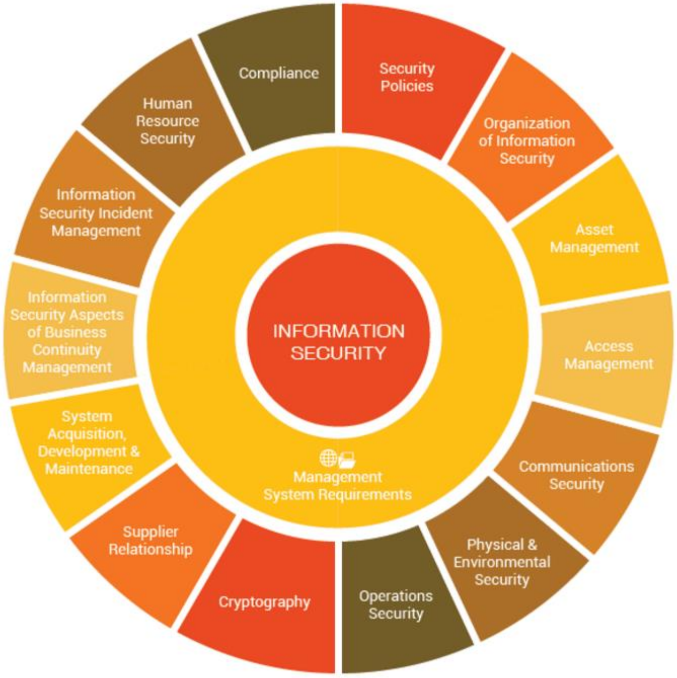
MOVEMENT

DATA THEFT

RESURRECTION

Pick an Industry Framework

ISO 27000

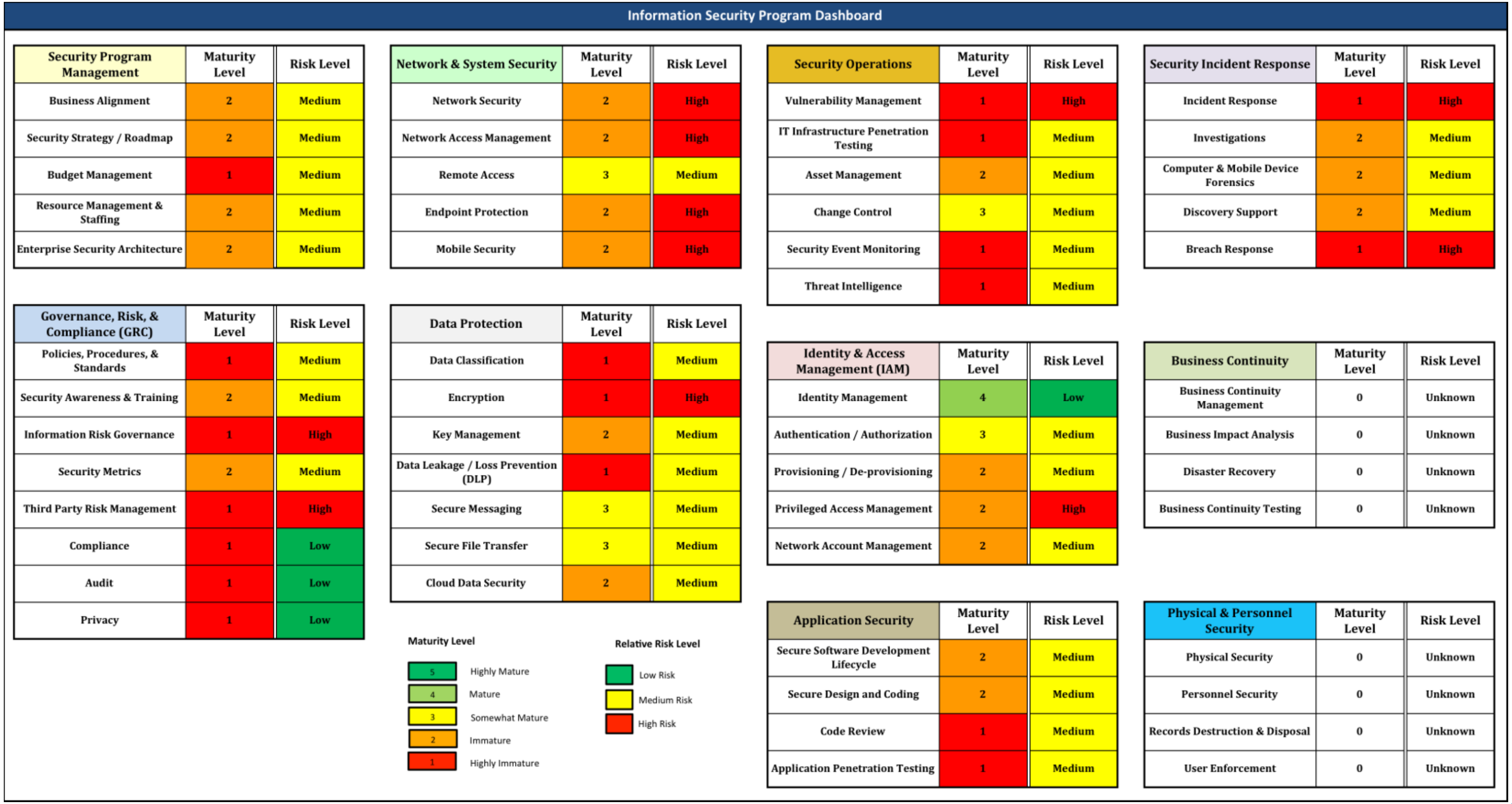


Compliance
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
INFORMATION SECURITY
Management System Requirements

NIST CSF

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anamolies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Assess Current Environment



Information Security Program Dashboard

Security Program Management	Maturity Level	Risk Level
Business Alignment	2	Medium
Security Strategy / Roadmap	2	Medium
Budget Management	1	Medium
Resource Management & Staffing	2	Medium
Enterprise Security Architecture	2	Medium

Network & System Security	Maturity Level	Risk Level
Network Security	2	High
Network Access Management	2	High
Remote Access	3	Medium
Endpoint Protection	2	High
Mobile Security	2	High

Security Operations	Maturity Level	Risk Level
Vulnerability Management	1	High
IT Infrastructure Penetration Testing	1	Medium
Asset Management	2	Medium
Change Control	3	Medium
Security Event Monitoring	1	Medium
Threat Intelligence	1	Medium

Security Incident Response	Maturity Level	Risk Level
Incident Response	1	High
Investigations	2	Medium
Computer & Mobile Device Forensics	2	Medium
Discovery Support	2	Medium
Breach Response	1	High

Governance, Risk, & Compliance (GRC)	Maturity Level	Risk Level
Policies, Procedures, & Standards	1	Medium
Security Awareness & Training	2	Medium
Information Risk Governance	1	High
Security Metrics	2	Medium
Third Party Risk Management	1	High
Compliance	1	Low
Audit	1	Low
Privacy	1	Low

Data Protection	Maturity Level	Risk Level
Data Classification	1	Medium
Encryption	1	High
Key Management	2	Medium
Data Leakage / Loss Prevention (DLP)	1	Medium
Secure Messaging	3	Medium
Secure File Transfer	3	Medium
Cloud Data Security	2	Medium

Identity & Access Management (IAM)	Maturity Level	Risk Level
Identity Management	4	Low
Authentication / Authorization	3	Medium
Provisioning / De-provisioning	2	Medium
Privileged Access Management	2	High
Network Account Management	2	Medium

Business Continuity	Maturity Level	Risk Level
Business Continuity Management	0	Unknown
Business Impact Analysis	0	Unknown
Disaster Recovery	0	Unknown
Business Continuity Testing	0	Unknown

Application Security	Maturity Level	Risk Level
Secure Software Development Lifecycle	2	Medium
Secure Design and Coding	2	Medium
Code Review	1	Medium
Application Penetration Testing	1	Medium

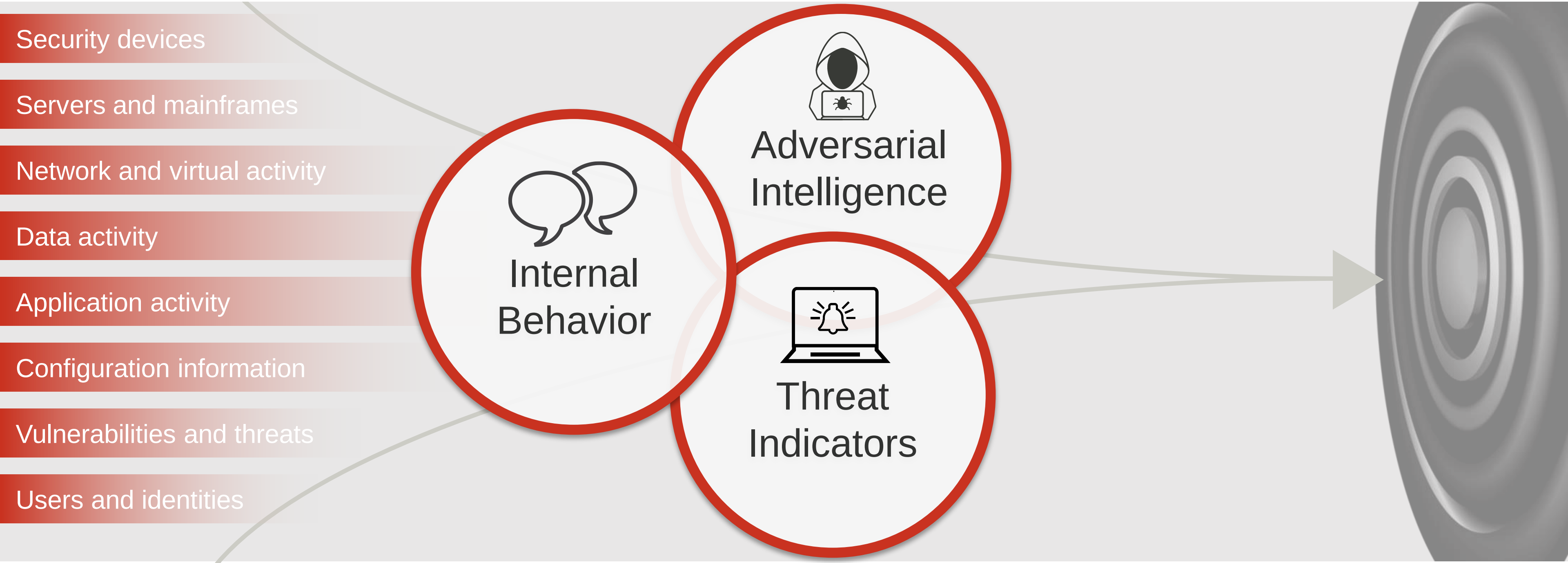
Physical & Personnel Security	Maturity Level	Risk Level
Physical Security	0	Unknown
Personnel Security	0	Unknown
Records Destruction & Disposal	0	Unknown
User Enforcement	0	Unknown

Maturity Level	
5	Highly Mature
4	Mature
3	Somewhat Mature
2	Immature
1	Highly Immature

Relative Risk Level	
🟩	Low Risk
🟨	Medium Risk
🟥	High Risk

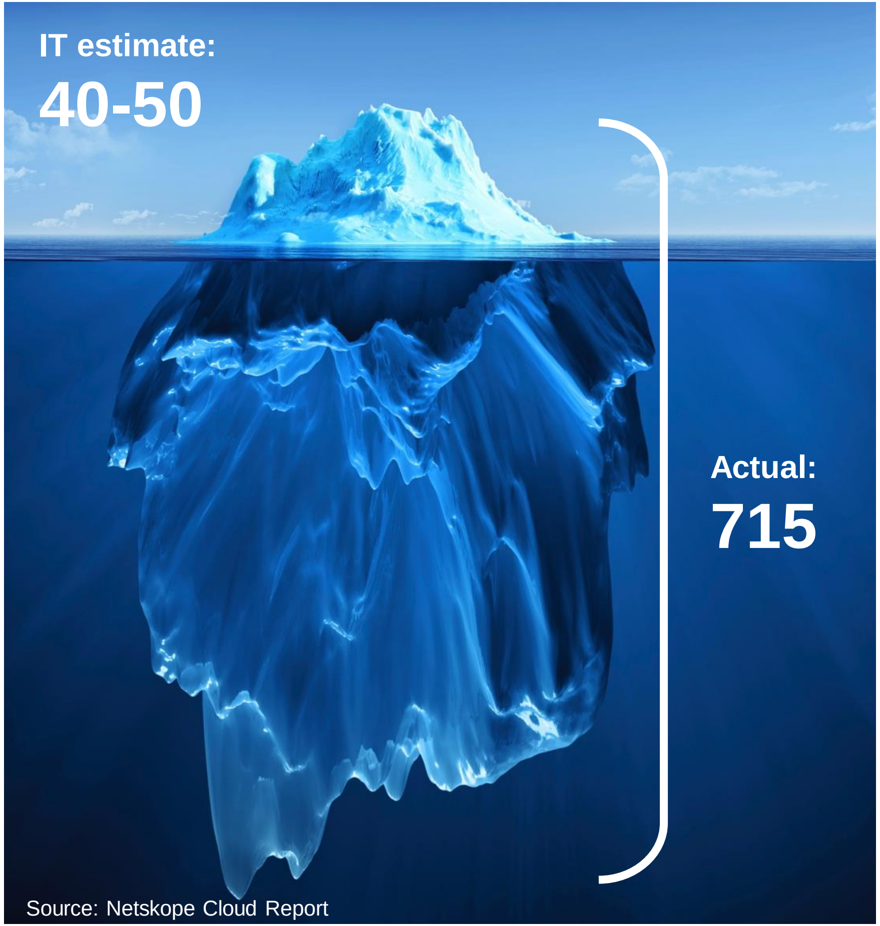
Don’t Overlook Emerging Practices and Technologies

Extensive Data Sources + Deep Threat Intelligence × Advanced Analytics = Knowledge



- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities

Can’t Simply Outsource Responsibility to the Cloud



Source: Netskope Cloud Report

Cloud procurement happens outside of IT

More than just Dropbox and Evernote. HR, finance, development, CRM, etc.

Little visibility or control, Requires oversight and a strategy

Cyber Insurance is Just Another Piece of the Puzzle

Errors & Omissions	Media	Network Security	Privacy
• Negligence or errors in your product or in the performance of your services • Failure to perform	• Infringement of intellectual property • Advertising and personal injury	• Unauthorized access • Transmission of malicious code • Data theft and destruction • Cyber extortion • Business interruption	PII/PHI data exposed by: • Hackers • Lost device • Rogue employees • Physical records

https://wsandco.com/cyber-liability/cyber-basics/

Don’t Ignore Compliance Obligations

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

HIPAA
Health Insurance Portability & Accountability Act

Sarbanes-Oxley
Financial and Accounting Disclosure Information

✓GLBA
COMPLIANCE

✓ SOC 2 TYPE II

✓ SOC 3

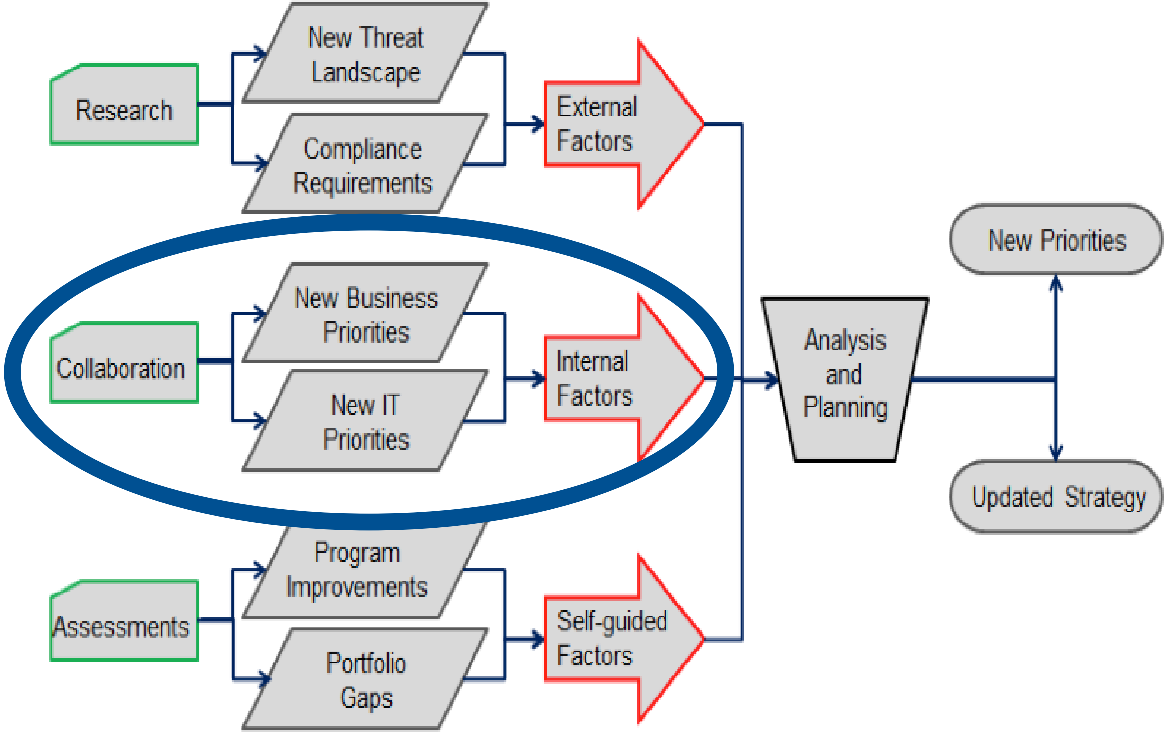
FFIEC
FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

FedRAMP SM

Pci

FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT

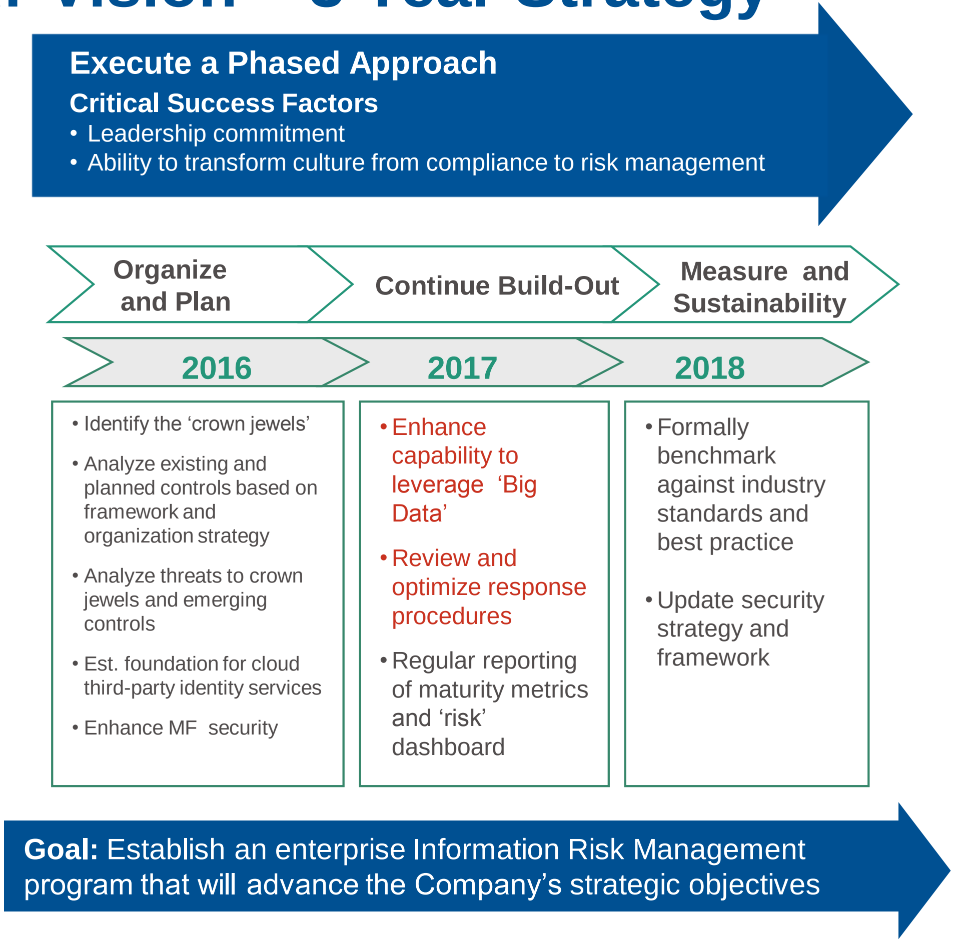
Time to Draft Strategy and Priorities



Enable Your Vision – 3 Year Strategy

Current State

1. Additional resourcing underway including role of Data Scientist
2. Documented strategy
3. Improved alignment with business units
4. Basic foundation across company:
   - Testing of vulnerabilities, configuration issues
   - Regular risk-based testing of applications
5. Enhanced detection and response of security incidents incl. fine-tuning, operational readiness
6. Policy and governance routines formalized



Execute a Phased Approach

Critical Success Factors

- Leadership commitment
- Ability to transform culture from compliance to risk management

Organize and Plan	Continue Build-Out	Measure and Sustainability
2016	2017	2018
Identify the ‘crown jewels’ Analyze existing and planned controls based on framework and organization strategy Analyze threats to crown jewels and emerging controls Est. foundation for cloud third-party identity services Enhance MF security	Enhance capability to leverage ‘Big Data’ Review and optimize response procedures Regular reporting of maturity metrics and ‘risk’ dashboard	Formally benchmark against industry standards and best practice Update security strategy and framework

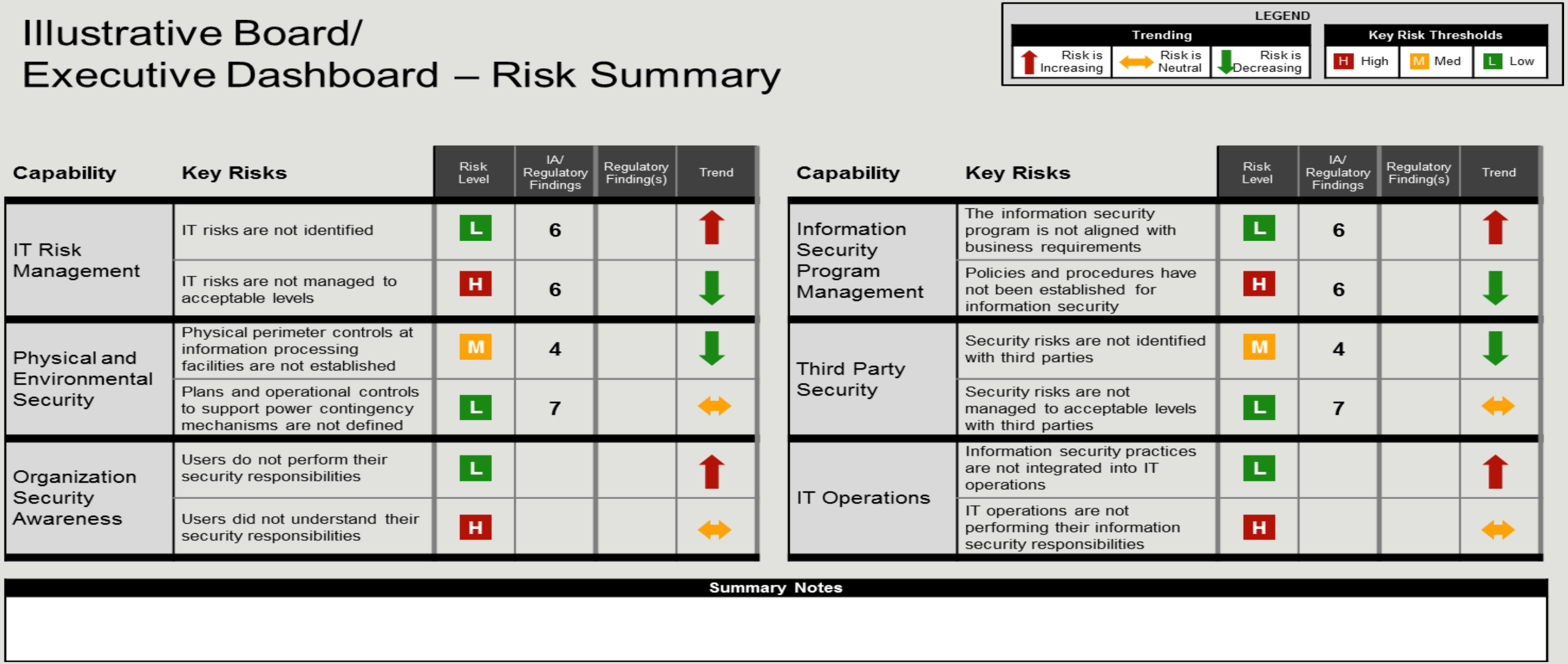
Goal: Establish an enterprise Information Risk Management program that will advance the Company’s strategic objectives

Future State

Efficient, effective management of risks by:

1. Program/costs aligned with business strategy and areas of highest risk
2. Information security program seen as a ‘business enabler’
3. Coordinated adoption of common policies, processes and technologies
4. Key processes automated
5. Formal controls and transparency with third parties, Cloud/SaaS
6. Early detection and remediation capabilities to minimize impact of internal/external attacks
7. Regular reporting

Scorecard – Regular Progress Reports



Illustrative Board/ Executive Dashboard – Risk Summary

LEGEND

Trending		
↑ Risk is Increasing	↔ Risk is Neutral	↓ Risk is Decreasing

Key Risk Thresholds		
H High	M Med	L Low

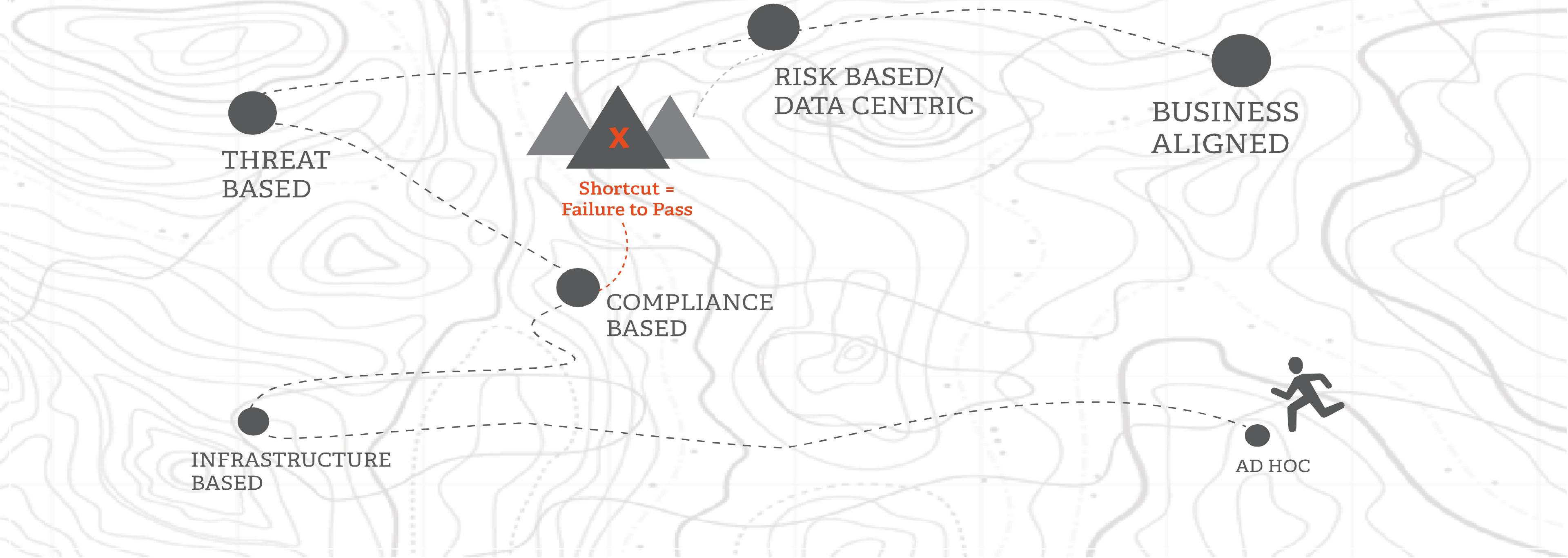
Capability	Key Risks	Risk Level	IA/ Regulatory Findings	Regulatory Finding(s)	Trend
IT Risk Management	IT risks are not identified	L	6		↑
	IT risks are not managed to acceptable levels	H	6		↓
Physical and Environmental Security	Physical perimeter controls at information processing facilities are not established	M	4		↓
	Plans and operational controls to support power contingency mechanisms are not defined	L	7		↔
Organization Security Awareness	Users do not perform their security responsibilities	L			↑
	Users did not understand their security responsibilities	H			↔

Capability	Key Risks	Risk Level	IA/ Regulatory Findings	Regulatory Finding(s)	Trend
Information Security Program Management	The information security program is not aligned with business requirements	L	6		↑
	Policies and procedures have not been established for information security	H	6		↓
Third Party Security	Security risks are not identified with third parties	M	4		↓
	Security risks are not managed to acceptable levels with third parties	L	7		↔
IT Operations	Information security practices are not integrated into IT operations	L			↑
	IT operations are not performing their information security responsibilities	H			↔

Summary Notes

The Security Journey

Business Aligned Strategy: Create a security program that enables the business by understanding the business objectives, compliance objectives, threats and material risks.



OPTIV

OPTIV

Brian Wrozek

Brian.Wrozek@Optiv.com

@bdwtexas