



Building an Effective Cyber Security Strategy

Office of the CISO



Agenda

Cyber Risk and Breach
Landscape



Leading Practices for Building an
Effective Cybersecurity Strategy



Increasing Demands and
Oversight Requires Focus

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)



Data Breaches and Records Exposed in 2016

JAVELIN +  **INSURANCE INFORMATION INSTITUTE** → \$16 B Stolen
15.4 M US Consumers

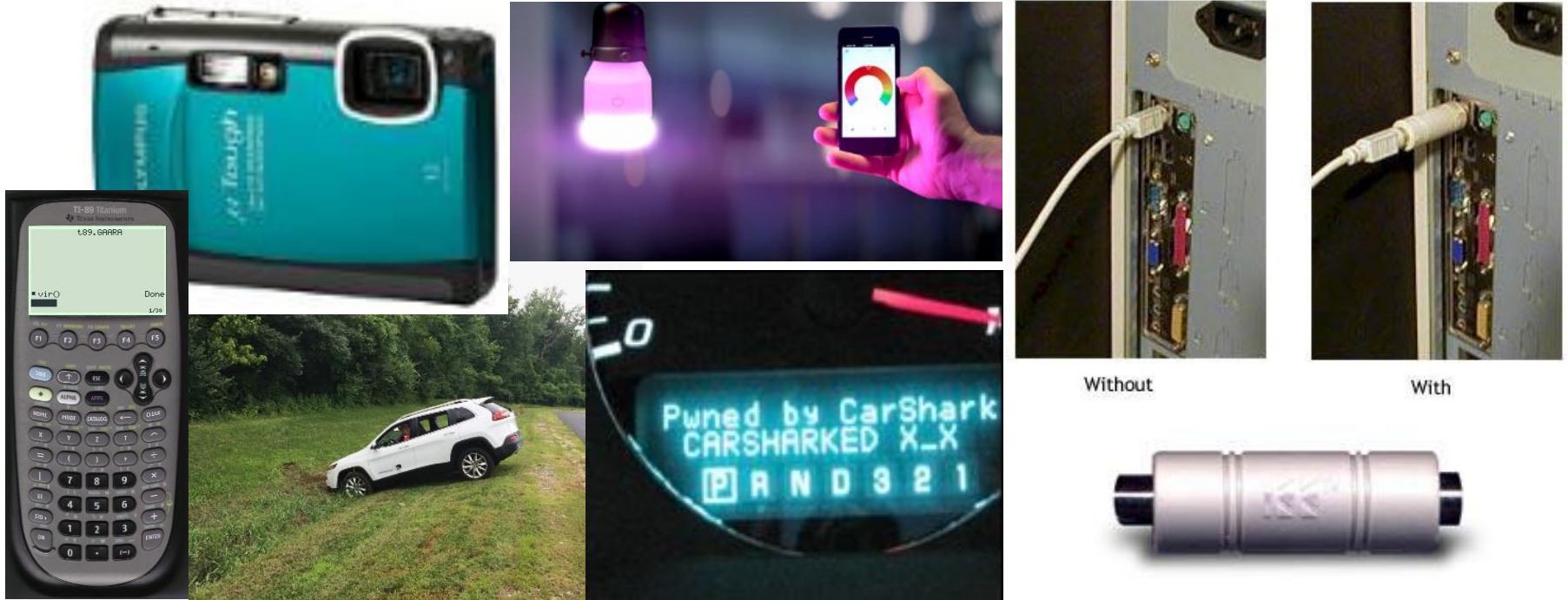
 **OTA**
Online Trust Alliance
DATA PRIVACY & PROTECTION DAY
2017 → 82,000 Incidents

 **RiskBased SECURITY** → 4,149 Breaches
4.2 B Records

 **ITRC** | **IDENTITY THEFT RESOURCE CENTER**
888.400.5530 → 1,093 Breaches

<https://www.riskbasedsecurity.com/2017/01/2016-reported-data-breaches-expose-over-4-billion-records/>
<https://otalliance.org/news-events/press-releases/consumer-data-breaches-level-while-other-incidents-skyrocket>
<http://www.idtheftcenter.org/2016databreaches.html>
<https://www.javelinstrategy.com/>

Stolen Records Are Only One Concern



Daily Headlines

Hack attack causes 'massive damage' at

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



Robert Siciliano Become a fan
Personal Security and Identity Theft Expert

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 uproar over a massive government breach, smaller companies continue to take recent cyberattacks as a warning. A restaurant chair system that provides a warning.

The announcement of a criminal hacker, a malicious software, the TV character Brewster, but sp

to steal personal financial data. Investigators have high confidence that Punkey received the network of an unidentified restaurant chain.

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.



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



Increasing Demands and Oversight Requires Focus

Five NACD Principles



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

NYDFS Cybersecurity Regulations

First-in-the-Nation Proposed Rule Aims to Protect Consumer Data and Financial Systems from Terrorist Organizations and Other Criminal Enterprises

Requirements – Deadline 8/28/2017

Cybersecurity Program and Documentation

Cybersecurity Policy and Incident Response Plan

Designate a CISO

Continuously Trained Cybersecurity Personnel

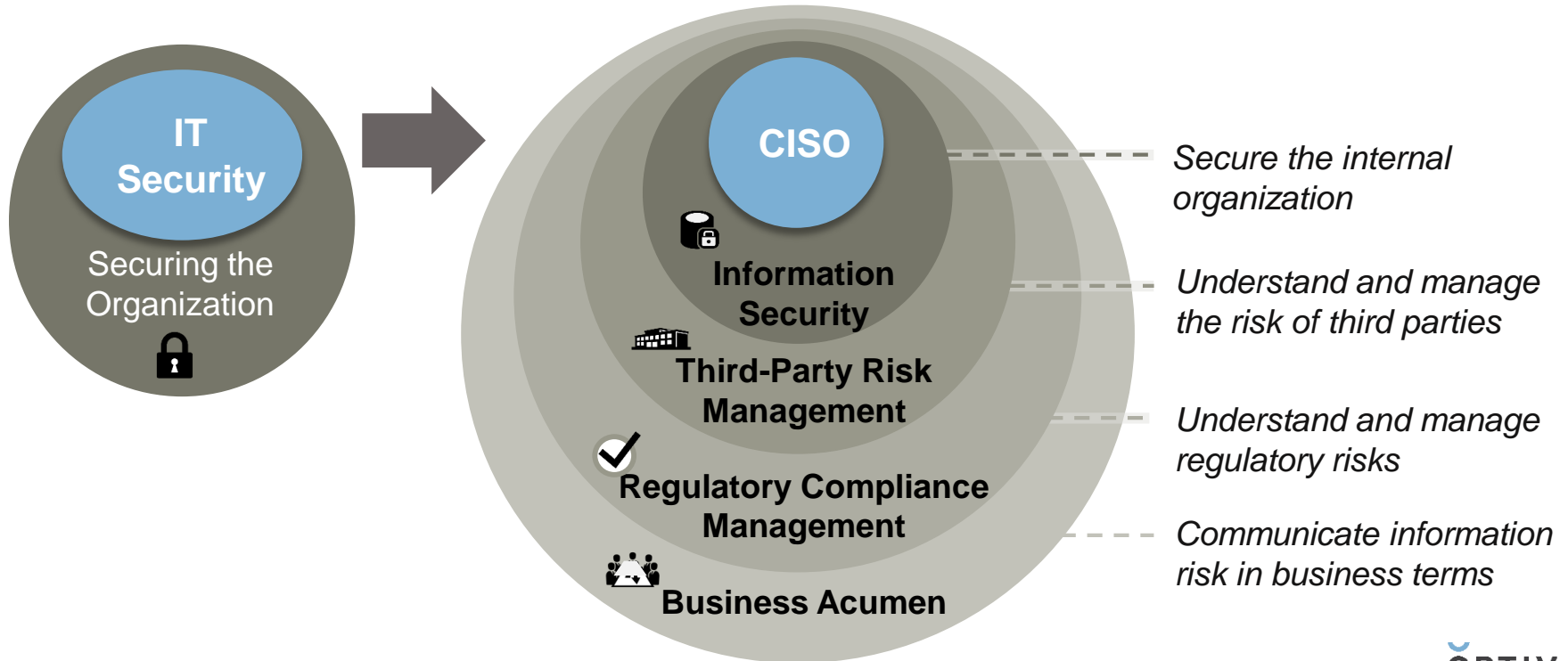
Limit Access Privileges

Notice of Cybersecurity Events to NYDFS (72 hrs)

Risk Assessment

Evolution of the CISO

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



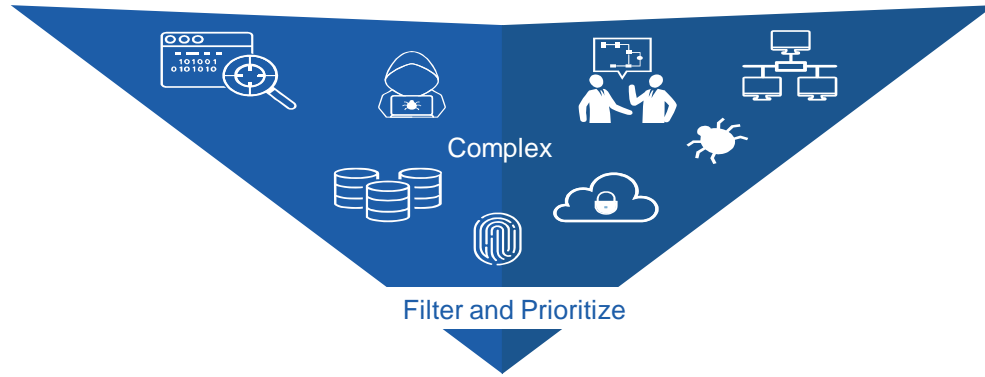
Problem Space Expands





Leading Practices for Building an Effective Cybersecurity Strategy

Business Aligned – Threat Aware Security Program



Focus on Business Critical Systems and Data



**Confidentiality,
Classification**



**Regulations,
Compliance**





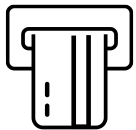


1000100101
11error001
0010001011



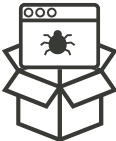

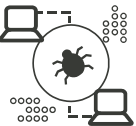
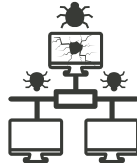


**Integrity,
Validity**



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

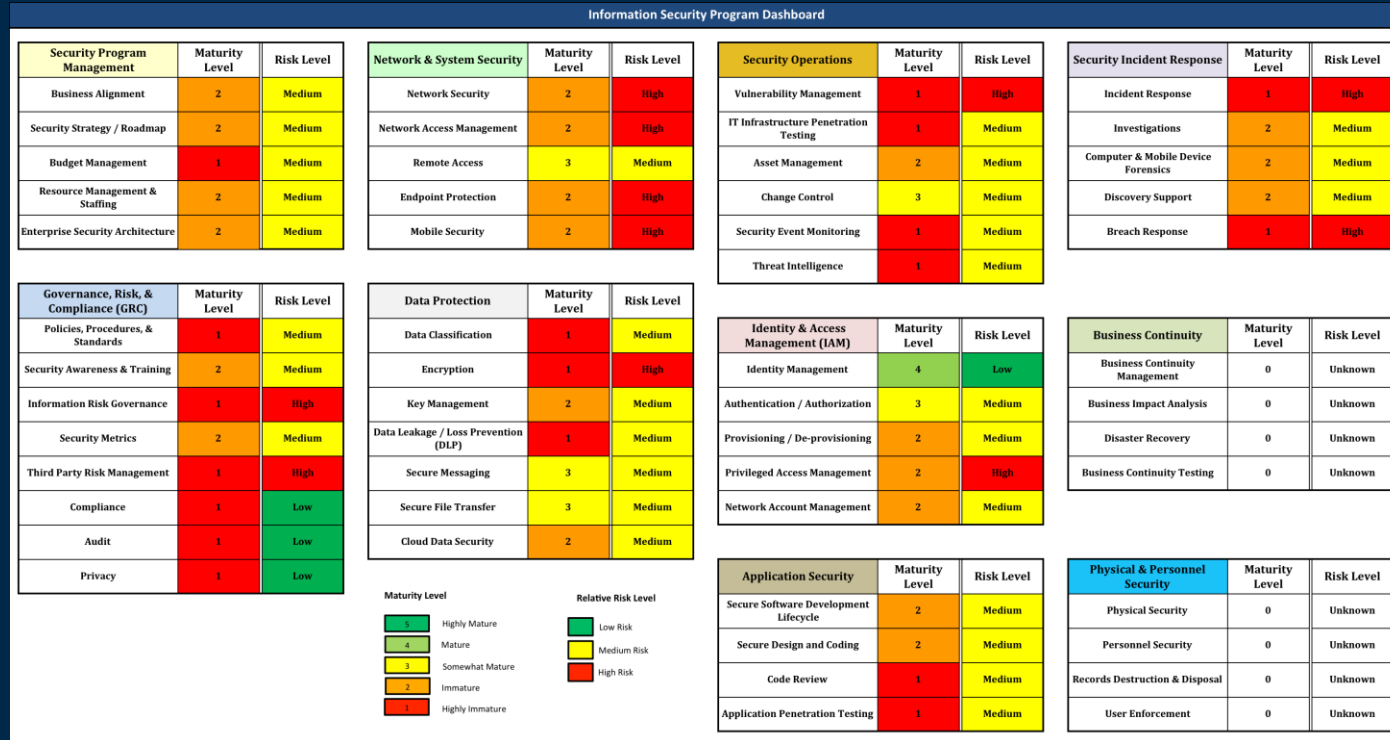
ISO 27000



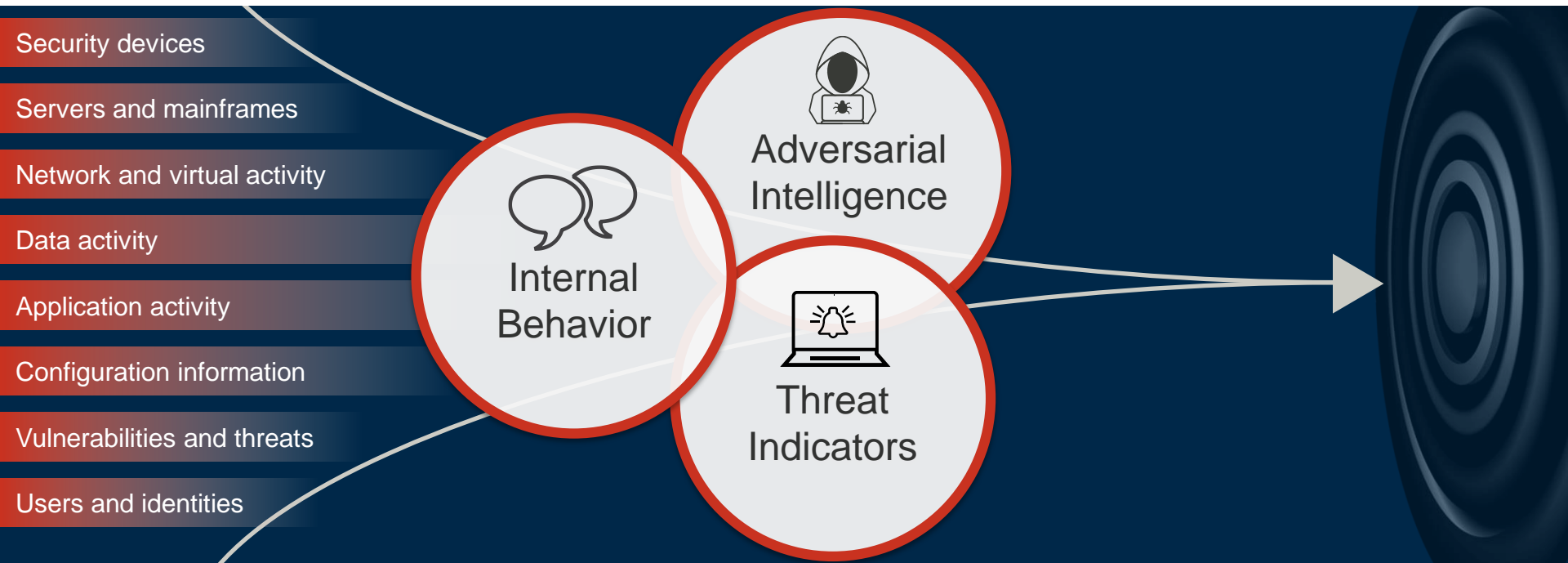
NIST CSF

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	Anomalies 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



Don't Overlook Emerging Practices and Technologies



Can't Simply Outsource Responsibility to the Cloud

IT estimate:

40-50



Actual:
715

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**

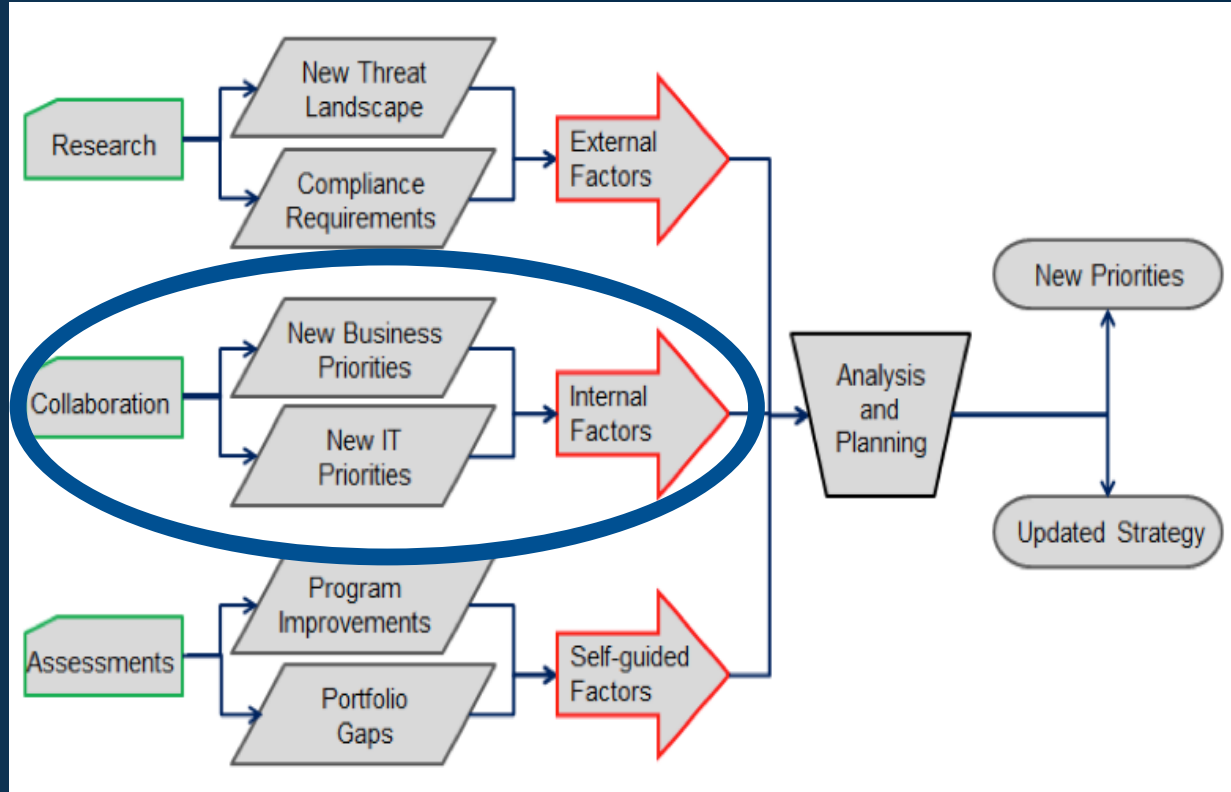
Cyber Insurance is Just Another Piece of the Puzzle

Errors and Omissions	Media	Network Security	Privacy
<ul style="list-style-type: none">• Negligence or errors in your product or in the performance of your services• Failure to perform	<ul style="list-style-type: none">• Infringement of intellectual property• Advertising and personal injury	<ul style="list-style-type: none">• Unauthorized access• Transmission of malicious code• Data theft and destruction• Cyber extortion• Business interruption	PII/PHI data exposed by: <ul style="list-style-type: none">• Hackers• Lost device• Rogue employees• Physical records

Don't Ignore Compliance Obligations



Time to Draft Strategy and Priorities



Enable Your Vision – 3 Year Strategy

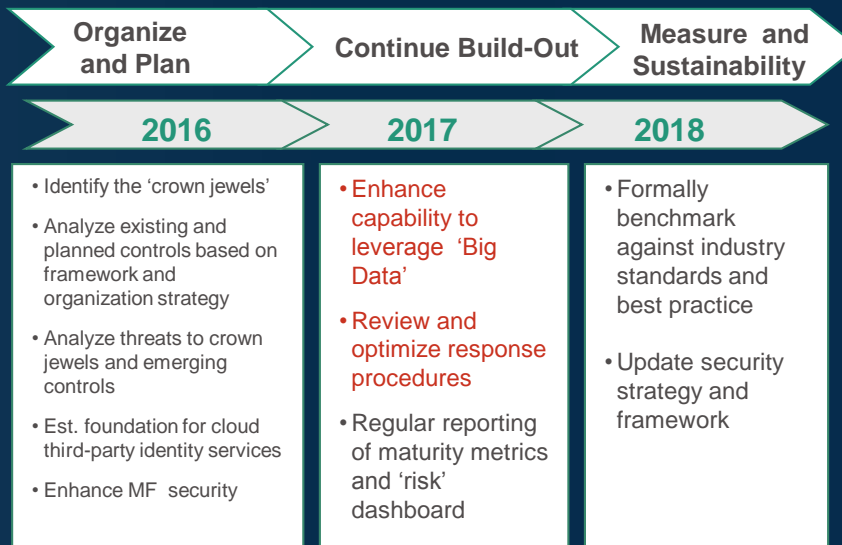
Current State

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



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

Trending			Key Risk Thresholds		
 Risk is Increasing	 Risk is Neutral	 Risk is Decreasing	 High	 Med	 Low

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

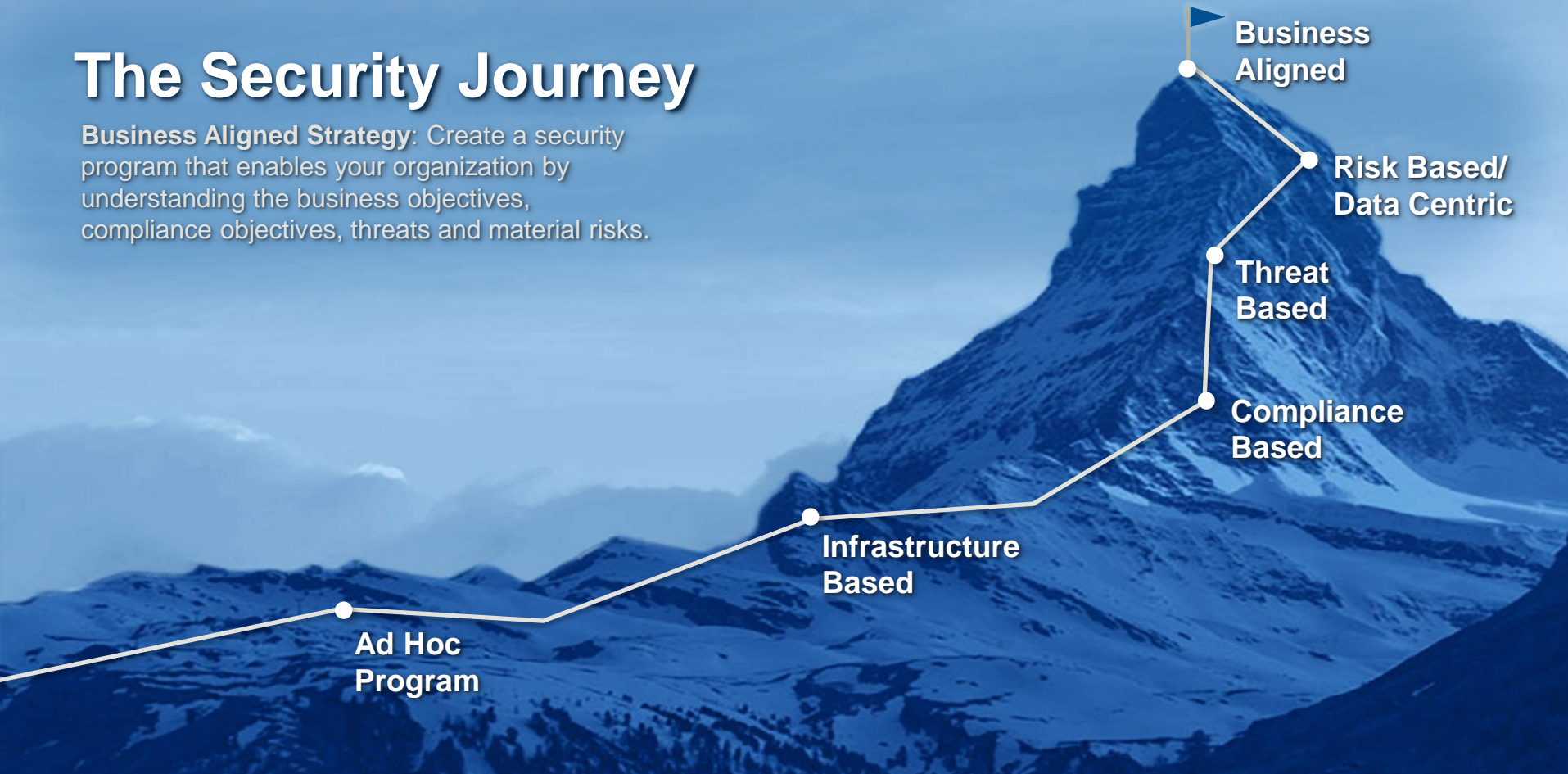
Capability	Key Risks	Risk Level	IA/ Regulatory Findings	Regulatory Finding(s)	Trend
Information Security Program Management	The information security program is not aligned with business requirements		6		
	Policies and procedures have not been established for information security		6		
Third Party Security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

Summary Notes

--

The Security Journey

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





Brian Wrozek

Brian.Wrozek@Optiv.com

@bdwtexas