



ISOAG Meeting

February 1, 2017

Welcome to CESC



Welcome and Opening Remarks

Michael Watson

February 1, 2017



ISOAG February 1, 2017 Agenda

- | | |
|--|---|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. Ideas how to conduct effective data sensitivity classifications, risk assessments, and IT Security Audits. | Peter Tsengas, Benjamin Sady, and John Richardson, Dixon Hughes Goodman LLP |
| III. Moving Beyond Compliance to a Risk-Based Approach to Cyber Security | Paige Pilarski & Nick Sanna, Risklens |
| IV. Commonwealth Vulnerability Scanning Initiative | Bill Freda, VITA |
| V. Upcoming Events | Mike Watson, VITA |
| VI. Partnership Update | Northrop Grumman |



DHG | risk advisory

COV InfoSec Compliance *Tips & Lessons Learned*

February 1, 2017

- Has your Agency felt like this when you see new IT Security compliance requirements coming your way?





- # Agenda
- IT System and Data Sensitivity Classification
 - Are we classifying IT Systems and Data correctly?
 - How can we improve our process for identifying sensitive IT Systems and Data?
 - IT Risk Assessment Process
 - Scoping
 - Risk Assessment Matrix
 - Reporting the Results
 - IT Security Audit Process
 - Scoping / Planning – demonstrate screen prints of the scoping matrix
 - Reporting – demonstrate screen prints of the report
 - Some Common Issues Across State Agencies



DHG | risk advisory

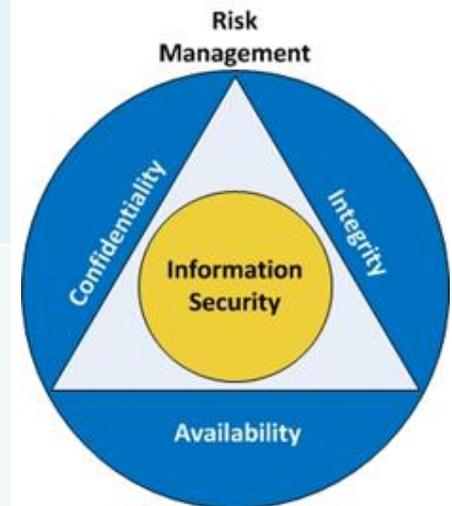
IT System and Data Sensitivity Classification Process

IT System and Data Sensitivity Classification Process

Correctly?

Basis for Data Sensitivity Classification

CIA Triad	Risks	Controls
Confidentiality	Unauthorized access to information and disclosure of information. Identity theft. Loss of privacy.	Encryption, Authentication, Access Controls, Security Monitoring Tools
Integrity	Unauthorized modification. Information is no longer reliable or accurate. Fraud.	Quality Assurance, Audit Logs, Database Triggers
Availability	Business disruption. Loss of customer confidence. Loss of revenue.	BCP Plans and Tests, Back-up Storage, Sufficient Capacity, Performance





IT System and Data Sensitivity Classification for identifying sensitive IT Systems and Data?

Example Data Sensitivity Classification Methodology

Information Types	Sensitivity Rating (High, Medium, Low)			Total Rating
	Confidentiality - C	Integrity - I	Availability - A	
Judicial Hearings	Med 2	Low 1	Low 1	Med 4
Income Information	Med 2	Med 2	Med 2	Med 6
Final System Rating & Classification	Med 2	Med 2	Med 2	Med 6
Overall System Impact: Medium				

Rating: (1 low, 2 med, 3 high);

Total Rating: 0-3 (low), 4-6 (med), 7-9 (high)

Overall System Impact: Average Total Ratings



DHG | risk advisory

IT Risk Assessment Process



- Scope of the Risk Assessment
- Risk Assessment Overview
- SEC501 Risk Assessment Matrix
- Reporting





Scoping the Risk Assessment

CNTL NO.	CONTROL NAME	VITA	Agency	System	IN SCOPE	REASON
AC-1	Access Control Policies		X		No	Agency Specific
AC-2	Account Management		X		No	Agency Specific
AU-2	Audit Events	X	X		No	VITA / Agency Specific
CM-2	Baseline Configuration	X			No	VITA hardens network appliances, servers, and workstations
IA-5	Authenticator Management			X	Yes	System specific



Agency

Risk Assessment Test Matrix Access Control (AC)

Prepared by:	
Date:	
Reviewed by:	
Date:	

Control #	Control	Risk Rating	Risk Procedure	Results	WP Reference	Conclusion
	A. The organization identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, service, application, guest/anonymous, and temporary.	High	Determine if individuals, groups, systems, services, application, guest/anonymous, and temporary accounts have been identified.			
	B. The organization assigns account managers for information system accounts.	High	Obtain and inspect a listing of all [System] users. Determine if account managers have been identified for service and application			

AC AT AU CA CM CP IA IR MA MP RA SA SC SI PL PE PS
Dates Proposed +

- Scoping the Risk Assessment
- Risk Assessment Takeaways
- Risk Assessment Matrix
- Reporting





DHG | risk advisory

IT Security Audit Process



The IT Security Audit Process

IT SECURITY AUDIT PROCESS

Overview

IT Audit – Methodology & Approach

Phase 1:
Familiarization

Phase 2:
Preliminary Survey &
Development of Audit Test
Plan

Phase 3:
Fieldwork & Completion of
IT Control Testing

Phase 4:
Reporting

Foundational Audit Methodologies: IIA, ISACA, COV Requirements

Status Reporting & Communication



IT Security Audit - Scoping / Planning

- Not every control in SEC 09 / SEC 05-01 can be covered in one of these audits
 - ITGC / Agency Level Controls
 - System Specific Controls
 - Risk Rating each Control – use NIST
- Rotation Control Families Strategy
 - Test all Technical Controls for multiple system in year 1
 - Test all Operational Controls for multiple systems in year 2
 - Test all Management Controls for multiple system in year 3
- Grouping Applications / Sensitive Systems Strategy
 - Some agencies have over 100 sensitive systems
 - If there are common platforms or infrastructures for multiples systems, consider testing them all together and treating them like 1 sensitive system audit report



IT Security Audit - Scoping /

- IT Security Audit Scoping Matrix Example

CNTL FAM.	CNTL NO.	CONTROL NAME	WD by VIT [^]	NIST PRIORITY	VITA	Agency	System	IN SCOPE FOR AUDIT	REASON
AC	AC-1	Access Control Policy and Procedures		P1		X		No	
AC	AC-2	Account Management		P1	X	X	X	Yes	<u>Agency:</u> - Network - ISO approves, VITA creates -Systems - centralized process for all systems <u>System:</u> ensure access is appropriate
AC	AC-2-COV					X	X	Yes	
AC	AC-3	Access Enforcement		P1		X	X	Yes	<u>Agency:</u> network devices, configs, and tools <u>System:</u> system specific
AC	AC-4	Information Flow Enforcement		P1			X	N/A	No external interfacing systems.
AC	AC-5	Separation of Duties		P1		X	X	Yes	<u>Agency:</u> network & centralized processes <u>System:</u> system specific
AC	AC-6	Least Privilege		P1		X	X	Yes	<u>Agency:</u> network & centralized processes <u>System:</u> system specific
AC	AC-7	Unsuccessful Logon Attempts		P2		X	X	Yes	<u>Agency:</u> network <u>System:</u> system specific
AC	AC-8	System Use Notification		P1		X		No	
AC	AC-8-COV					X		No	
AC	AC-9	Previous Logon (Access) Notification	WD	P0				N/A	
AC	AC-10	Concurrent Session Control	WD	P3				N/A	



IT Security Audit - Scoping /

- IT Security Audit Scoping Matrix Example – Planning

CNTL FAM.	CNTL NO.	CONTROL NAME	WD by VITA	NIST PRIORITY	VITA	Agency	System	IN SCOPE FOR AUDIT	REASON
AT	AT-1	Security Awareness and Training Policy and Procedures		P1		X		No	
AT	AT-2	Security Awareness Training		P1		X		No	
AT	AT-2-COV					X		No	
AT	AT-3	Role-Based Security Training		P1		X	X	No	Agency: Network, ISO System: admins Test this at agency level
AT	AT-4	Security Training Records		P3		X	X	No	Agency: Network, ISO System: admins Test this at agency level
AT	AT-5	Contacts with Security Groups and Associations	WD	---				N/A	
AU	AU-1	Audit and Accountability Policy and Procedures		P1		X		No	
AU	AU-2	Audit Events		P1		X	X	Yes	Agency: network System: system
AU	AU-3	Content of Audit Records		P1		X	X	Yes	Agency: network System: system
AU	AU-4	Audit Storage Capacity		P1		X	X	Yes	Agency: network System: system
AU	AU-5	Response to Audit Processing Failures		P1		X	X	Yes	Agency: network System: system
AU	AU-6	Audit Review, Analysis, and Reporting		P1		X	X	Yes	Agency: network System: system
AU	AU-7	Audit Reduction and Report Generation	WD	P2					



IT Security Audit - Scoping / Planning

- IT Security Audit Scoping Matrix Example –

CNTL FAM.	CNTL NO.	CONTROL NAME	WD by VIT^	NIST PRIORITY	VITA	Agency	System	IN SCOPE FOR AUDIT	REASON
CA	CA-1	Security Assessment and Authorization Policies and Procedures		P1		X		No	
CA	CA-2	Security Assessments	WD	P2				N/A	
CA	CA-3	Information System Interconnections		P1			X	Yes	
CA	CA-3-COV						X	Yes	
CA	CA-4	Security Certification	WD	---					
CA	CA-5	Plan of Action and Milestones	WD	P3					
CA	CA-6	Security Authorization		P2			X	Yes	
CA	CA-7	Continuous Monitoring		P2		X		No	
CA	CA-8	Penetration Testing	WD	P2					
CA	CA-9	Internal System Connections	WD	P2					
CM	CM-1	Configuration Management Policy and Procedures		P1		X		No	
CM	CM-2	Baseline Configuration		P1			X	Yes	
CM	CM-2-COV						X	Yes	
CM	CM-3	Configuration Change Control		P1		X	X	Yes	Agency: network and devices System: in scope
CM	CM-3-COV					X	X	Yes	Agency: network and devices System: in scope
CM	CM-4	Security Impact Analysis		P2			X	Yes	
CM	CM-5	Access Restrictions for Change		P1		X	X	No	
CM	CM-6	Configuration Settings		P1		X		No	
CM	CM-7	Least Functionality		P1			X	Yes	
CM	CM-8	Information System Component Inventory		P1			X	Yes	



IT Security Audit Reporting

- What Should Agencies Include in the IT Security Audit Report?

- Executive Summary
- Overview of Agency and Systems Being Audited
- Audit Objective, Scope and Methodology
- Audit Findings and Recommendations



IT Security Audit - Reporting

- Should we include Audit Ratings in our reports?

- Report / System Rating – Satisfactory, Needs Improvement, Unsatisfactory, etc.
- Issue Rating – High, Medium, Low



IT Security Audit Report Example

Table of Contents

EXECUTIVE SUMMARY.....	1
OVERVIEW OF AGENCY AND SYSTEMS.....	3
AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY	4
AUDIT FINDINGS AND RECOMMENDATIONS	7



EXECUTIVE SUMMARY

System Name

In this section provide a brief background description of the system for which the IT Security Audit is being performed.

Why We Performed This Audit

System Name has been classified as "sensitive" applications in accordance with Commonwealth of Virginia (COV) IT Security Standard (SEC501-09), and as such are required to be audited under the COV Information Security Audit Standard (SEC502-02.2).

Audit Objectives and Scope

Our procedures were performed during the period of **Start Date** through **End Date** and were designed with an objective to assess the effectiveness of the SEC501-09 – IT Security Standard controls, applicable to the **System Name**, included within these control families:

- Access Control
- Security Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Planning
- Personnel Security
- Risk Assessment
- System & Services Acquisition
- System and Communication Protection
- System and Information Integrity



IT Security Audit Report Example -

Summary Results

In this section provide the overall audit conclusion, and summarize the audit findings below

Agency IT General Control Findings

- Summarize any general IT control findings identified during the audit in this section.

System Name Specific Findings

- Summarize any system specific IT control findings identified during the audit in this section.

Implementing all of the recommendations in this audit will add value to **Agency Name** by strengthening the security controls that protect their application and associated data.

Methodology

To complete the IT Security Audit requirements outlined by **Agency Name**, DHG's audit process was aligned with the following Virginia Information Technologies Agency (VITA) Standards:

- IT Security Audit Standard (SEC502-02.2)
- IT Security Audit Guideline (SEC512-01)

The DHG audit process was broken down into the below four phases, as summarized in the table below:

Phase	Phase Objectives	Tasks
Phase 1: Familiarization	To obtain an understanding of applicable laws, policies, procedures and best practices impacting the agency.	Conduct initial research and review of laws, policies, procedures and best practices impacting the Authorized User's systems and/or processes being audited as per the contract.
Phase 2: Preliminary Survey and Development of Audit Test Plan	<p>To adequately plan the audit & obtain background information for the activities to be audited including researching past reports, applicable laws, policies and standards as well as best practices.</p> <p>To obtain an understanding of the IT System area being audited including goals & objectives, regulations, & areas of management concern.</p>	<p>This phase will include performance of the following tasks:</p> <ul style="list-style-type: none"> • Detail information gathering phase which may include reviews of <ul style="list-style-type: none"> ○ procedures, ○ diagrams, ○ the systems boundary definition, ○ risk assessment and ○ other existing documentation • Interviews and/or survey key personnel, • Perform walkthroughs and observations, • Identify and perform an initial

Example -



Sample -

Overall, based on our procedures performed, **Agency Name** appears to have adequately implemented COV ITRM SEC501-09 IT Security Standard requirements for each of the in-scope controls. However, we noted a few areas of improvement that management should consider, to further strengthen the internal controls around the **System Name**. The detailed conditions noted for these areas of improvement are listed below:

Agency IT General Control Findings

1. General IT Control Finding 1

Detail:

State the finding detail in this section, including any references to the specific SEC501-09 IT Security Standard requirement (e.g., COV ITRM SEC501-09 Section Reference: AT-04 (A.))

Risk:

Summarize any risks that may arise as a result of the finding.

Recommendation:

State your audit recommendation to address the finding in this section.

System Name Findings

1. System Specific IT Control Finding 1

Detail:

State the finding detail in this section, including any references to the specific SEC501-09 IT Security Standard requirement (e.g., COV ITRM SEC501-09 Section Reference: AT-04 (A.))

Risk:

Summarize any risks that may arise as a result of the finding.

Recommendation:

State your audit recommendation to address the finding in this section.



IT Security Audit - Common Issues Across Agencies

- Remember you are not alone out there!!!

Agencies





Recap

- IT System and Data Sensitivity Classification Process Takeaways
- Risk Assessment Process Takeaways
- IT Security Audit Process Takeaways



Thank You!

Ben Sady
Director
IT Risk Advisory Services
Ben.Sady@dhgllp.com
804.474.1267

Peter Tsengas
Lead Consultant
IT Risk Advisory
Services
Peter.Tsengas@dhgllp.com
804.474.1293

John Richardson
Lead Consultant
IT Risk Advisory Services
John.Richardson@dhgllp.com
804.474.1221



RISKLENS PRESENTATION



CYBER RISK = BUSINESS RISK

EXPECTATIONS FOR CISOs HAVE CHANGED



EXPECTATIONS FOR CISOs HAVE CHANGED



THE COMMUNICATION CHALLENGE

CFO

“How much loss exposure do we have? Are we spending too little or too much on mitigation?”

ERM

“Do we have enough cyber insurance?”

BOARD/CEO

“We don’t want to be the next news headline cybercrime victims. Are we doing enough to minimize risk?”

CIO

“Are we spending our cybersecurity budget on the right things?”

CISO

“Έχουμε πάνω από δέκα χιλιάδες τρωτά σημεία , είναι συμβατό με το ογδόντα τοις εκατό”

EASIER SAID **THAN DONE...**

1 Qualitative Checklists & Excel

NIST



The way most cybersecurity professionals measure risk today fails to quantify cyber-risk in terms the business can understand and use

2 Governance, Risk & Compliance Tools

~~GRC~~



GRADE **C-**

Average CISO self assessment on their cyber risk reporting.

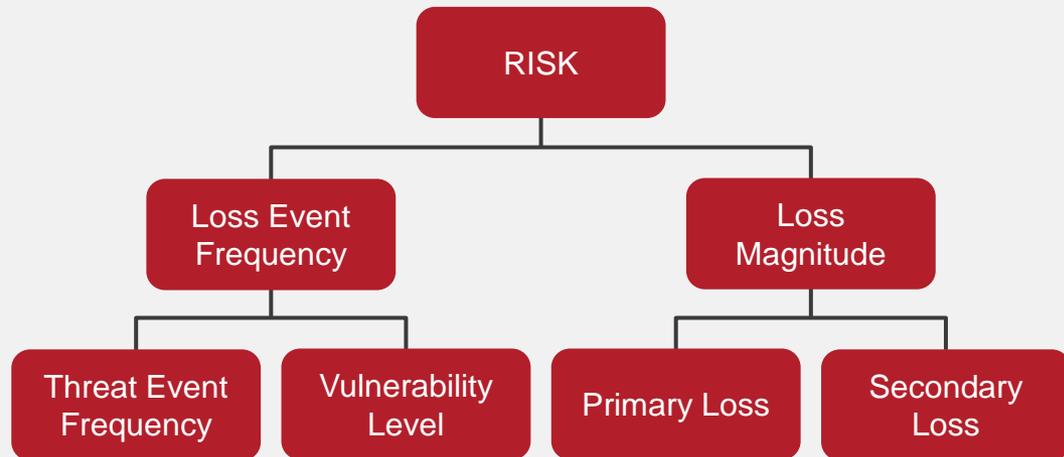
Source: Global survey of 100 executives in 2013 by the World Economic Forum and McKinsey & Co.

THE BREAKTHROUGH

A UNIQUELY SCALABLE RISK MODEL

FAIR

Factor Analysis
of Information Risk



Accredited as an
Industry Standard by



Complementary to
Risk Frameworks



Supported by a Fast
Growing Community

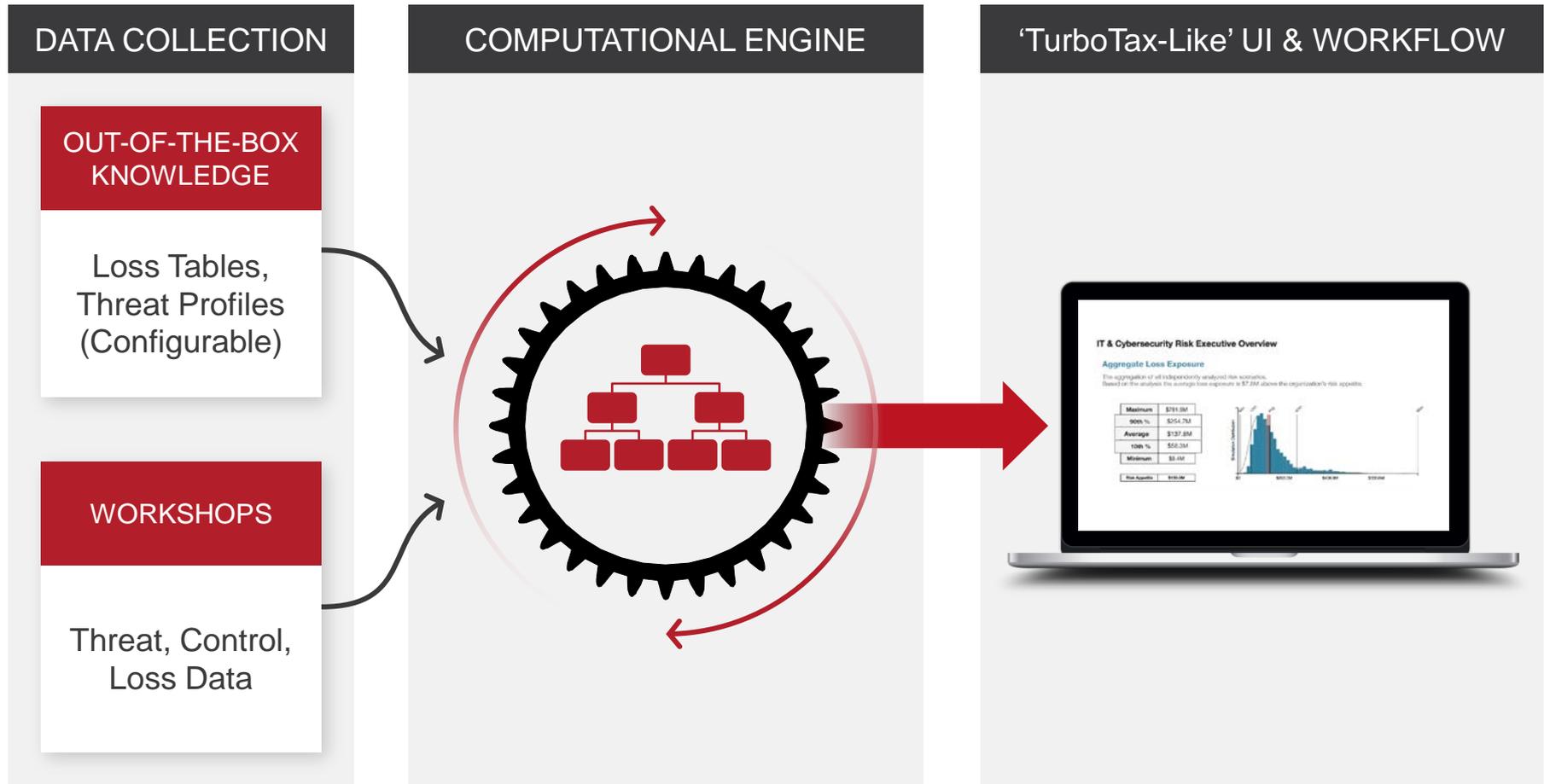


FAIR Book Inducted
in Cybersecurity Canon

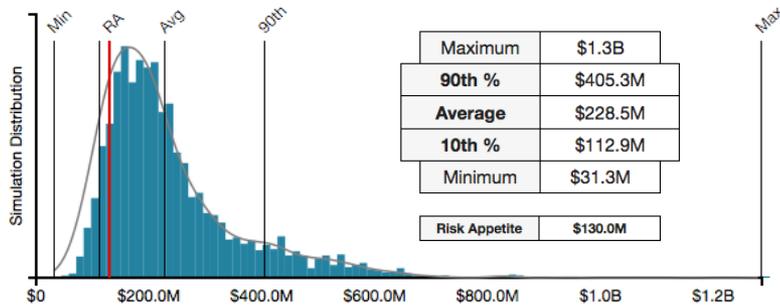


PURPOSE BUILT SOFTWARE

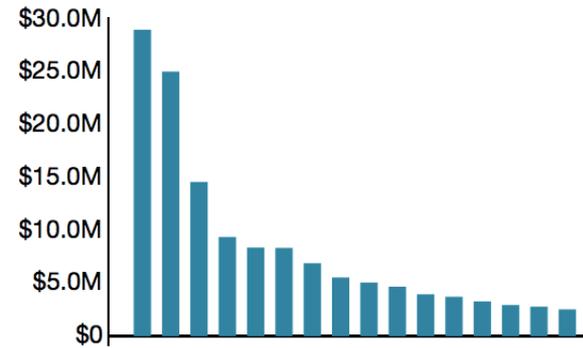
The only cyber risk quantification platform purpose-built on FAIR



“HOW MUCH RISK DO WE HAVE?”

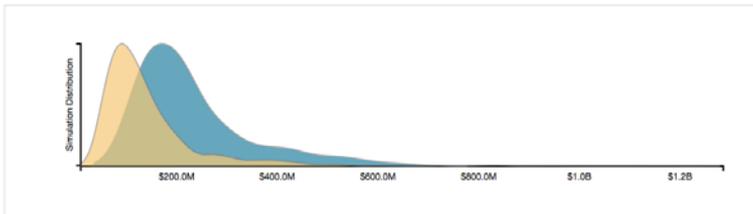


“WHAT ARE OUR TOP RISKS?”



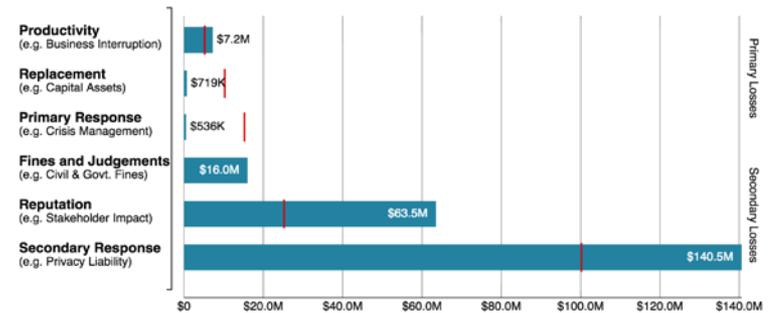
“HAVE WE REDUCED RISK?”

Loss Exposure Distributions

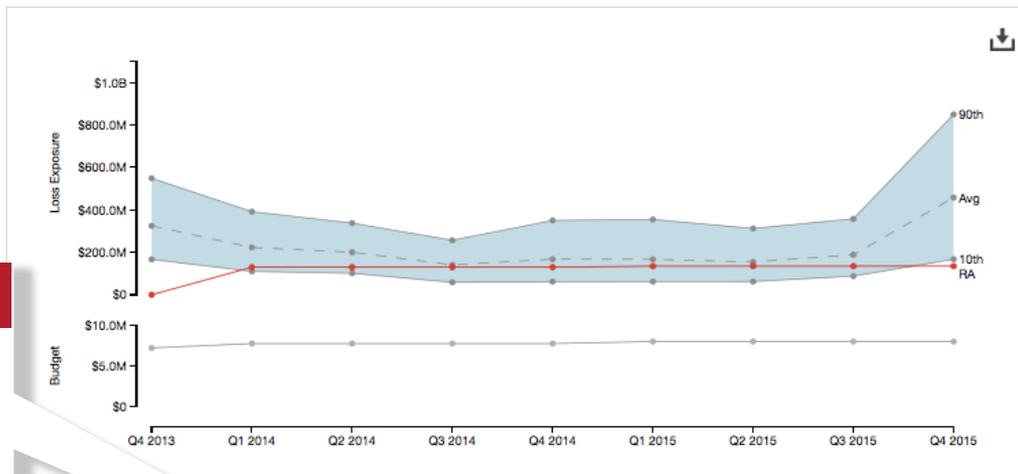


Analysis	Reporting Period	Minimum	10th %	Average	90th %	Maximum	
Annual Baseline Enterprise Analysis	Quarter 1 2014	\$31.3M	\$112.9M	\$228.5M	\$405.3M	\$1.3B	✘
Quarterly Updated Enterprise Analysis	Quarter 3 2014	\$9.4M	\$58.3M	\$137.8M	\$254.7M	\$781.5M	✘

“WHAT TYPE OF LOSS CAN WE EXPECT?”



“HOW IS RISK TRENDING VS. OUR RISK APPETITE?”



INFOSEC BUDGET

By how much did we reduce risk over time?

RISK APPETITE

What is the risk appetite approved by the board?

EMERGING THREATS

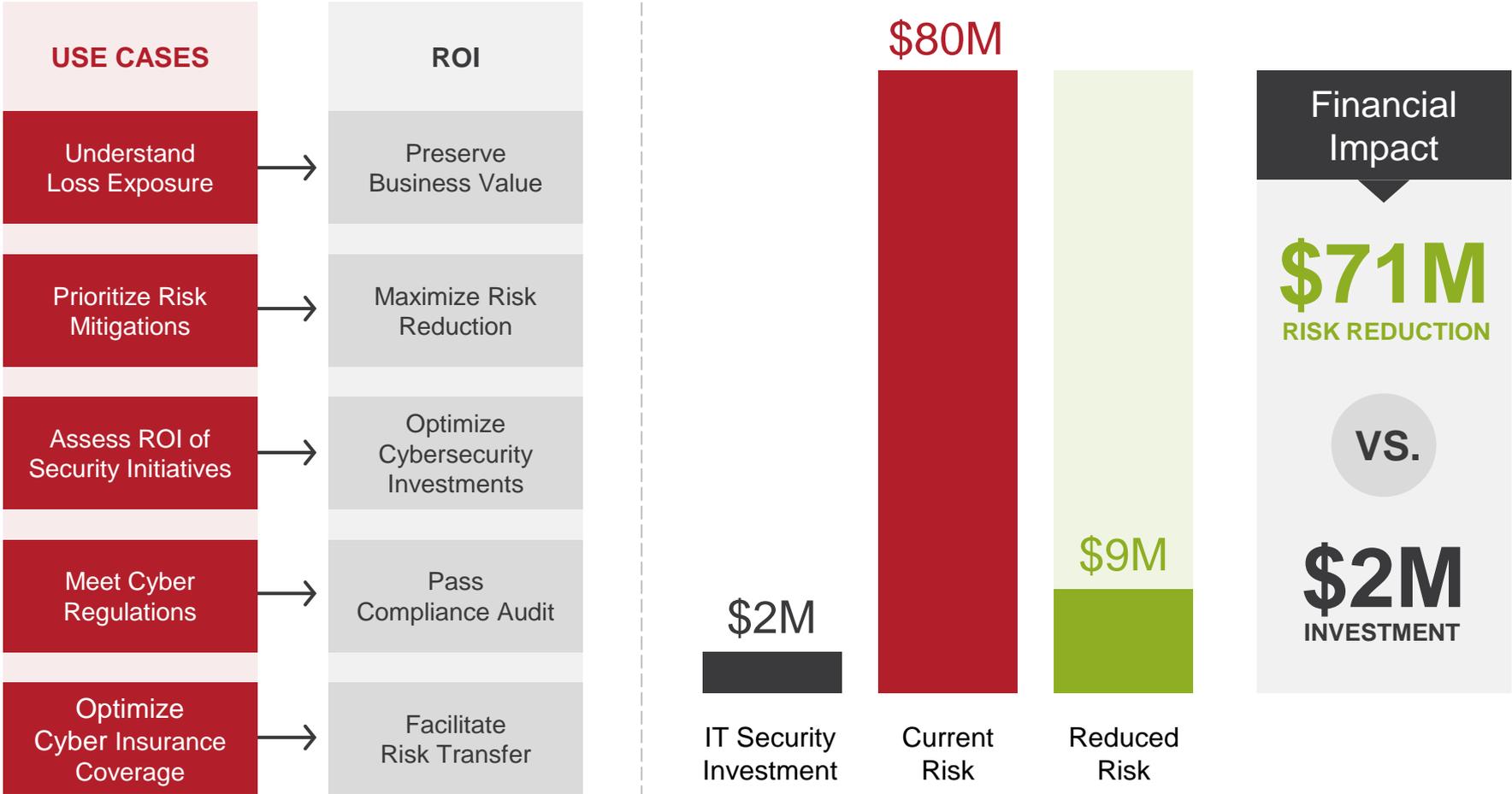
What is the effect of this new threat?

Reporting Period	Analysis	Loss Exposure			Budget		Risk Appetite	
		10th	Average	90th	CapEx	OpEx		
Q4 2013	Quarterly Enterprise Analysis	\$166.9M	\$324.5M	\$548.8M	\$2.5M	\$4.7M	\$0	View
Q1 2014	Quarterly Enterprise Analysis	\$112.6M	\$223.1M	\$391.6M	\$2.8M	\$5.0M	\$130.0M	View
Q2 2014	Quarterly Enterprise Analysis	\$101.4M	\$200.5M	\$337.6M	\$2.8M	\$5.0M	\$130.0M	View
Q3 2014	Quarterly Enterprise Analysis	\$59.0M	\$140.7M	\$256.9M	\$2.8M	\$5.0M	\$130.0M	View
Q4 2014	Quarterly Enterprise Analysis	\$62.1M	\$167.8M	\$350.2M	\$2.8M	\$5.0M	\$130.0M	View
Q1 2015	Quarterly Enterprise Analysis	\$62.4M	\$167.1M	\$354.7M	\$3.0M	\$5.0M	\$135.0M	View
Q2 2015	Quarterly Enterprise Analysis	\$62.5M	\$154.5M	\$312.4M	\$3.0M	\$5.0M	\$135.0M	View
Q3 2015	Quarterly Enterprise Analysis	\$88.0M	\$188.6M	\$357.7M	\$3.0M	\$5.0M	\$135.0M	View
Q4 2015	Quarterly Enterprise Analysis	\$167.6M	\$457.8M	\$849.5M	\$3.0M	\$5.0M	\$135.0M	

M&A

Are we OK in taking on this much cyber risk through M&A?

MULTIPLE DIMENSIONS OF ROI



NEW CYBER RISK MGMT. STANDARDS

“The agencies are seeking to develop a consistent, repeatable method to support the ongoing quantification of cyber risk of covered entities.”*

“We are familiar with the FAIR quantification model (...) and are considering building upon these methodologies.”

ANPR - * Federal Reserve, OCC, FDIC – Oct. 19, 2016

Assessment of overall exposure to cyber risk

Approval by the board of the risk appetite

Reduction of risk to board-approved level

Quantitatively measure ability to reduce risk



CYBER RISK ECONOMICS IS HERE





There are no slides for
Bill Freda's presentation
due to security reasons.





Virginia Information Technologies Agency

Upcoming Events





OSIG Training

Course: Integrating Cybersecurity in SDLC

Instructor: David Cole / SysAudits Inc.

Location: CESC

Dates: Feb 14-15, 2017

CPE: 16.0 hours

Price: \$350

<https://osig.virginiainteractive.org>

10100



VirginiaTech

Invent the Future[®]

Advanced Security Essentials - Enterprise Defender

March 6-11, 2017 ■ Torgersen Hall ■ Virginia Tech ■ Blacksburg, VA

- VT is hosting SANS SEC 501:
“Advanced Security Essentials
-Enterprise Defender”
 - Dates: 3/6 – 3/11
 - Location: VT, Blacksburg
(will also be available in simulcast)
- Huge discounts for State/Local
 - For more information:
 - www.cpe.vt.edu/isect



Future ISOAG

March 1, 2017 1:00 - 4:00 pm @ CESC

**Speaker: Mike Howard, Assistant Director, IS Audits
US House of Representatives OIG**

Speaker: Karen Cole & John Brightly, Assura, Inc

Speaker: Jason Ancarrow, IT Security Director, CARMAX

ISOAG meets the 1st Wednesday of each month in 2017



Virginia Information Technologies Agency



Registration is Open

COV Information Security Conference

Richmond, VA

2017

“Expanding security knowledge”



April 13 & 14

Contact: CovSecurityConference@vita.virginia.gov



COV Security Conference

More information on the 2017 COV Information Security conference can be found @:

<http://www.vita.virginia.gov/default.aspx?id=6442472001>

Questions concerning the conference can be emailed to:

CovSecurityConference@vita.virginia.gov

Keynote Speakers



April 13 – Day One

John W. Martin, President and CEO of SIR

John W. Martin is the president and CEO of SIR, Inc. a 52-year-old marketing research and consulting firm headquartered in Richmond, Virginia.

Keynote Speaker



April 14 – Day Two

Arnold E. Bell - CISO

Arnold joined SLAIT consulting as Chief Information Security Officer and Director of Security Solutions in January 2015. He brings over 27 years of security experience to SLAIT.

ADJOURN

THANK YOU FOR ATTENDING

