Richard Dorough

Richard Dorough, EnCE, C-CISO, CIPP, CGEIT, CISA
Managing Director, Forensic Technology Solutions
Fort Worth, TX

Mr. Dorough re- joined PricewaterhouseCoopers in 2012 and has over 19 years experience in IT Security, IT Forensics, IT Audit, and IT Governance. Areas of focus include digital threat assessments, Cyber incident identification and response, electronic investigations and IT Security organization assessment and development.

Prior to returning to PwC, Mr. Dorough was the Global Chief Information Security Officer for Textron. As Global Chief Information Security Officer, Mr. Dorough was responsible for developing, maintaining and assuring continuous improvement of Textron's Information Technology Security strategy, programs, policies and processes. This included leadership of the Information Technology Risk Management (ITRM) Council which is a team of Security leaders from across Textron's Business Units and COEs. Mr. Dorough was also responsible for IT Privacy governance, software asset management, disaster recovery and led the IT portion of the electronic discovery (eDiscovery) program for Textron.

Mr. Dorough has a Bachelor of Science in Computer Science from the University of Texas at Tyler. He is a certified DFSS Green Belt and has additional certifications in IT, IT Forensics, IT Data Privacy, eDiscovery, IT Audit, and IT Security. He is recognized as an industry SME in the area of IT, IT Security, eDiscovery and Forensics and frequently speaks at security related events, functions and conferences and sits on several security related boards and governing bodies. CIO Talk Radio, CXO Magazine, CSO perspectives, CISO Executive Summit to name a few.

Matthew Wilson

Matthew Wilson
Director, IT Risk, Security and Privacy
Dallas, TX

Matt is a Dallas based PwC Risk Assurance Director with 10 years of experience specializing in IT, Risk and Security. Matt has held a number of internal and external audit leadership positions across many industries. Matt has been responsible for risk assessment, audit plan development and execution, leading business process and compliance reviews, ERP system assessments, system implementation assurance reviews, SSAE16 reporting, and other internal and external audit engagements. In this capacity Matt has developed significant experience with IT risk assessment, system implementation assurance and information security.

Ashley Shugart

Ashley Shugart
Manager, IT Risk, Security and Privacy
Dallas, TX

Ashley Shugart is a Security & Privacy Services Manager specializing in privacy, data protection and information security. His privacy service delivery experience ranges from basic policy reviews, training/awareness development, benchmark analysis, privacy impact assessments and developing and implementing national and global privacy programs. Ashley's primary focus revolves around leading practices with an emphasis on program development, regulatory compliance, incident response management, and operational implementation. He also has extensive knowledge of privacy frameworks (e.g., Generally Accepted Privacy Principles) and the ever-evolving legal, regulatory and compliance landscape.

Ashley also advises clients on security best practices and requirements in order to safeguard corporate assets, including confidential data, intellectual property, and sensitive data such as credit card and health related information. He has a broad understanding of technology, its role in the enterprise and the tools, techniques and processes required to mitigate technology risks. Ashley has performed a variety of security related services including program strategy and policy development, IT governance, incident response and handling, baseline assessment and benchmarking reviews, as well as experience with HIPAA, NIST, COBIT, and ISO27002.

In today's ever-changing glossary of terminology in this area, Ashley has direct experience in areas of privacy compliance, data protection, IT security, data classification, privacy strategy, privacy program management.

www.pwc.com/cybersecurity

Cybersecurity: Recent Data Breaches and the Evolving Role of Internal Audit

Presented to the Association of Government Accountants Dallas Chapter

October 16, 2014

pwc

Recent statistics - today, security compromises are a persistent—and globally pervasive—business risk

• The US government notifies **3,000 companies** that they were were attacked and charges nation-backed hackers with economic espionage.

• Compromises of retailers culminate in a recent breach of **56 million credit cards**.

• Heartbleed defect results in the **loss of 4.5 million** healthcare records.

• Powerful malware **infects hundreds of energy companies** worldwide.

• More than half of **global securities exchanges** are hacked.

• **Regulators around the world** are beginning to more proactively address cyber risks.

Source: PwC's The Global State of Information Security Survey 2015

The number of security incidents continues to soar

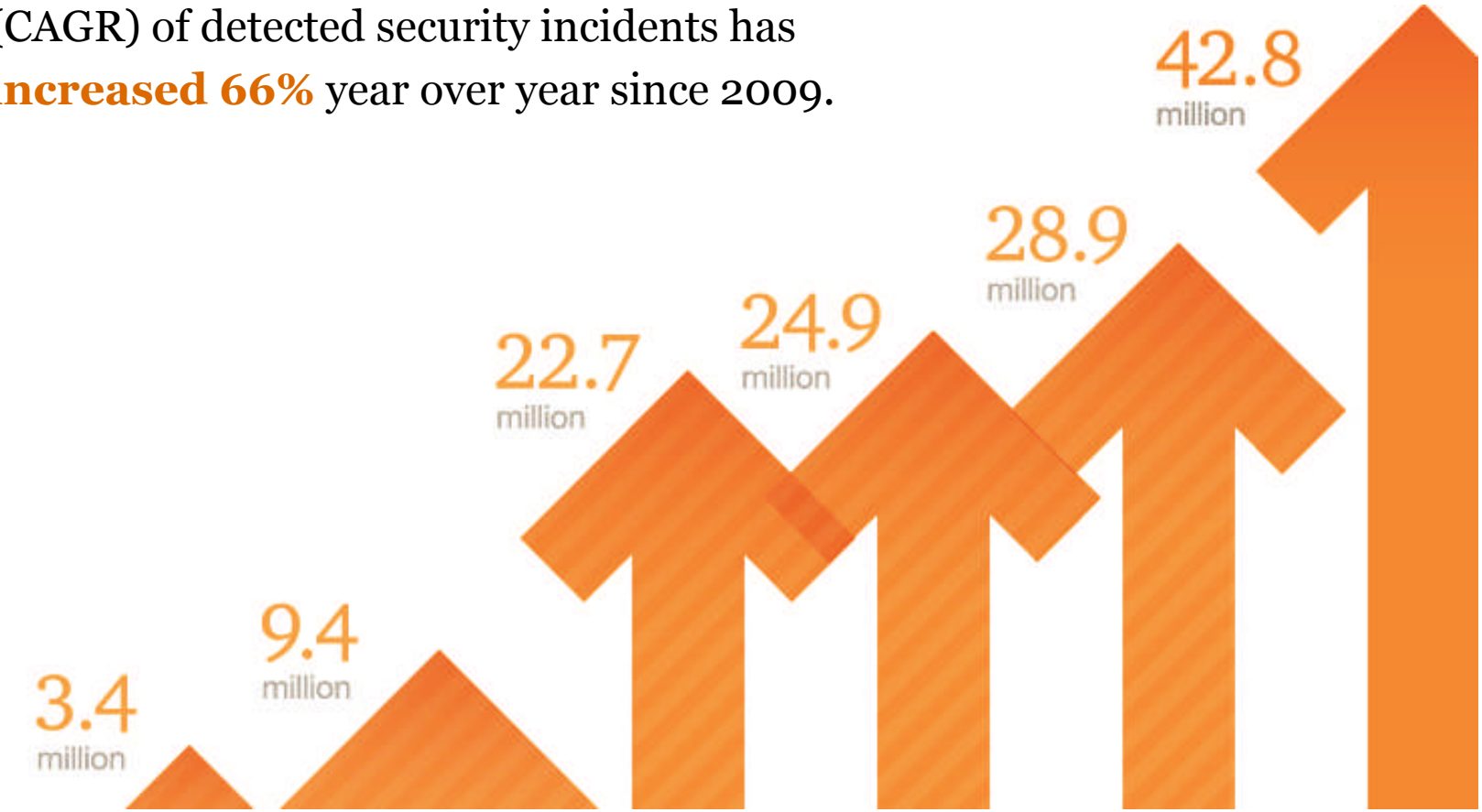
The total number of security incidents detected by survey respondents climbed to **42.8 million** this year, an increase of 48% over 2013.

It's the equivalent of 117,339 incoming attacks *per day, every day*. And that's just the compromises that were discovered.

Source: PwC's The Global State of Information Security Survey 2015

A steady 66% year-over-year growth since 2009

Taking a longer view, our survey data shows that the compound annual growth rate (CAGR) of detected security incidents has **increased 66%** year over year since 2009.



Source: PwC's The Global State of Information Security Survey 2015

Primary Failure points

#4 Underestimating Technology

3 Underestimating Data

2 Senior Management Commitment

1 Maturity and Execution of Company IT Security Tools and Capabilities

Profile of threat actors

Adversary	Motives	Targets	Impact
Nation State	• Economic, political, and/or military advantage	• Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure	• Loss of competitive advantage • Disruption to critical infrastructure
Organized Crime	• Immediate financial gain • Collect information for future financial gains	• Financial / Payment Systems • Personally Identifiable Information • Payment Card Information • Protected Health Information	• Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
Hacktivists	• Influence political and /or social change • Pressure business to change their practices	• Corporate secrets • Sensitive business information • Information related to key executives, employees, customers & business partners	• Disruption of business activities • Brand and reputation • Loss of consumer confidence
Insiders	• Personal advantage, monetary gain • Professional revenge • Patriotism	• Sales, deals, market strategies • Corporate secrets, IP, R&D • Business operations • Personnel information	• Trade secret disclosure • Operational disruption • Brand and reputation • National security impact

Anatomy of a cyber attack

Recon	Weaponize	Deliver	Exploit	Install	C2	Actions
Target an organization or industry	**Craft malicious payload**	**Payload sent to target**	**Compromise system**	**Installation of malware / tools post exploitation**	**Command and control**	**Ultimate goals achieved**
• *Browse websites* • *Social Media* • *Pre social engineering* • *External scans*	• *Trojanized docs* • *Packed executables* • *Obfuscated shell code*	• *SQL injection* • *Spear phishing*	• *Execution of payload* • *Critical phase of the attack.*	• *Install rootkits* • *Password crackers* • *Keyloggers* • *Hacking tools*	• *Leverage exploit* • *Access backdoors* • *Reverse shell* • *Lateral movement* • *Maintain persistence*	• *Exfiltrate data* • *Launch other attacks*

Real-Time Monitoring of the Cyber Kill Chain

Phase	Detect	Deny	Disrupt	Degrade	Deceive
Reconnaissance	NIDS, Web analytics	Firewall ACL			
Weaponize	NIDS, In-line AV	NIPS			
Delivery	In-line AV, User Awareness	Proxy filter	In-line AV	Queuing	
Exploitation	HIDS	Patch	DEP		
Installation	HIDS	Whitelist	AV		
C2	NIDS, In-line AV	Firewall ACL	NIPS	Tarpit	DNS redirect
Actions	HIDS, DLP	DLP		Quality of Service	Honeypot

Evolving business risks…

…impacting brand, competitive advantage, and shareholder value

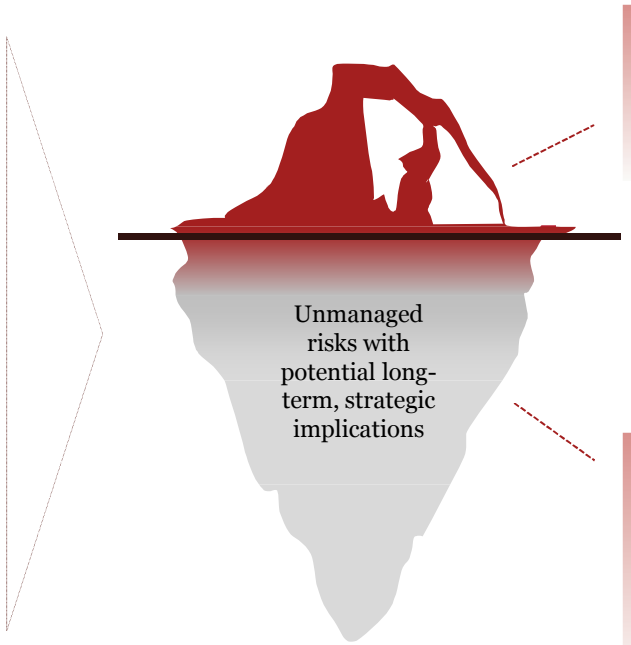
Highlights of activities impacting risk:

Advancements in and evolving use of technology – *adoption of cloud-enabled services; Internet of Things ("IoT") security implications; BYOD usage*

Value chain collaboration and information sharing – *persistent 'third party' integration; tiered partner access requirements; usage and storage of critical assets throughout ecosystem*

Operational fragility – *Real-time operations; product manufacturing; service delivery; customer experience*

Business objectives and initiatives – *M&A transactions; emerging market expansion; sensitive activities of interest to adversaries*



Historical headlines have primarily been driven by compliance and disclosure requirements

However, the real impact is often not recognized, appreciated, or reported

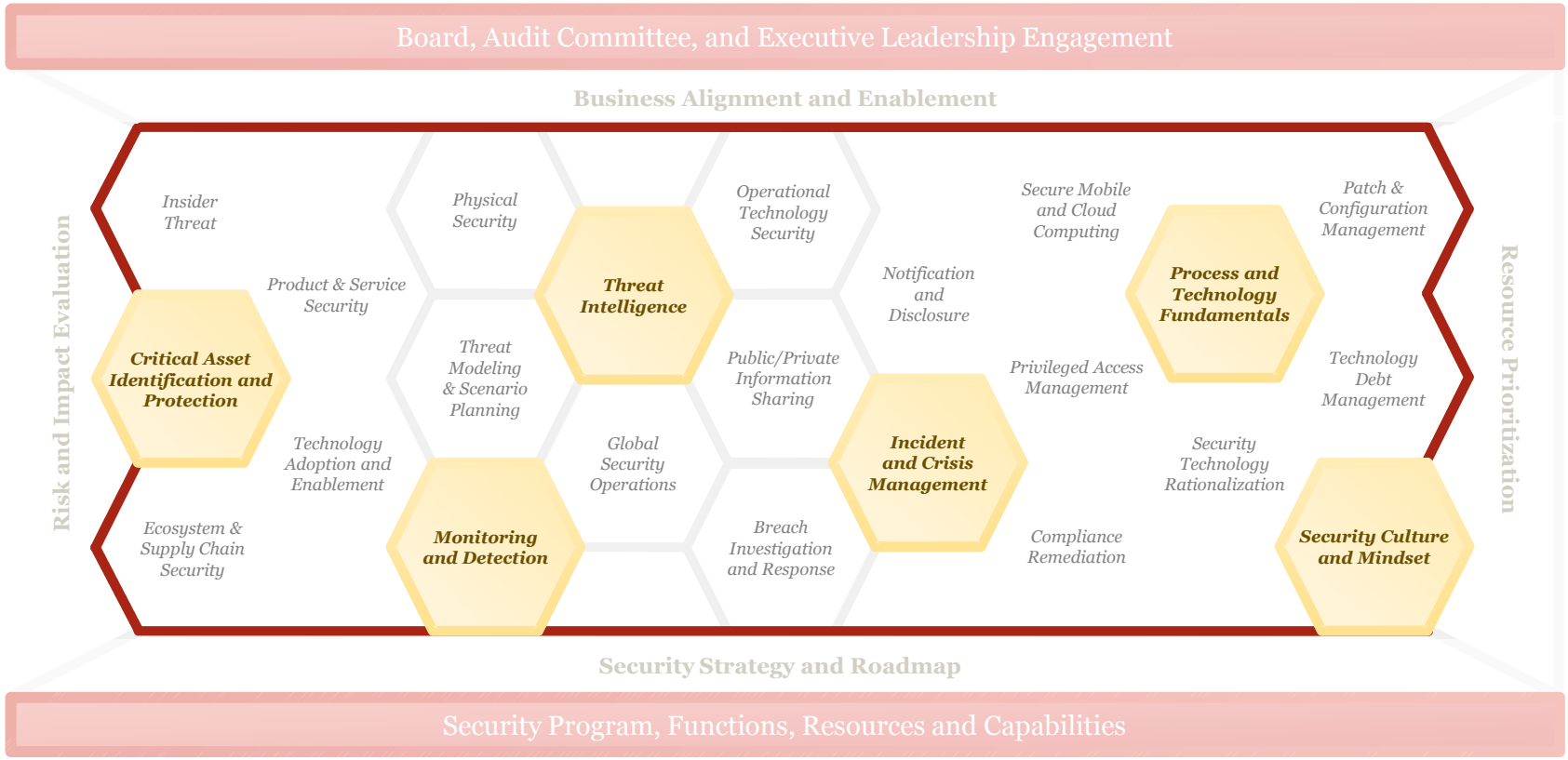
Cybersecurity must be viewed as a strategic business imperative in order to protect brand, competitive advantage, and shareholder value

Enterprise risks associated with cybercrime

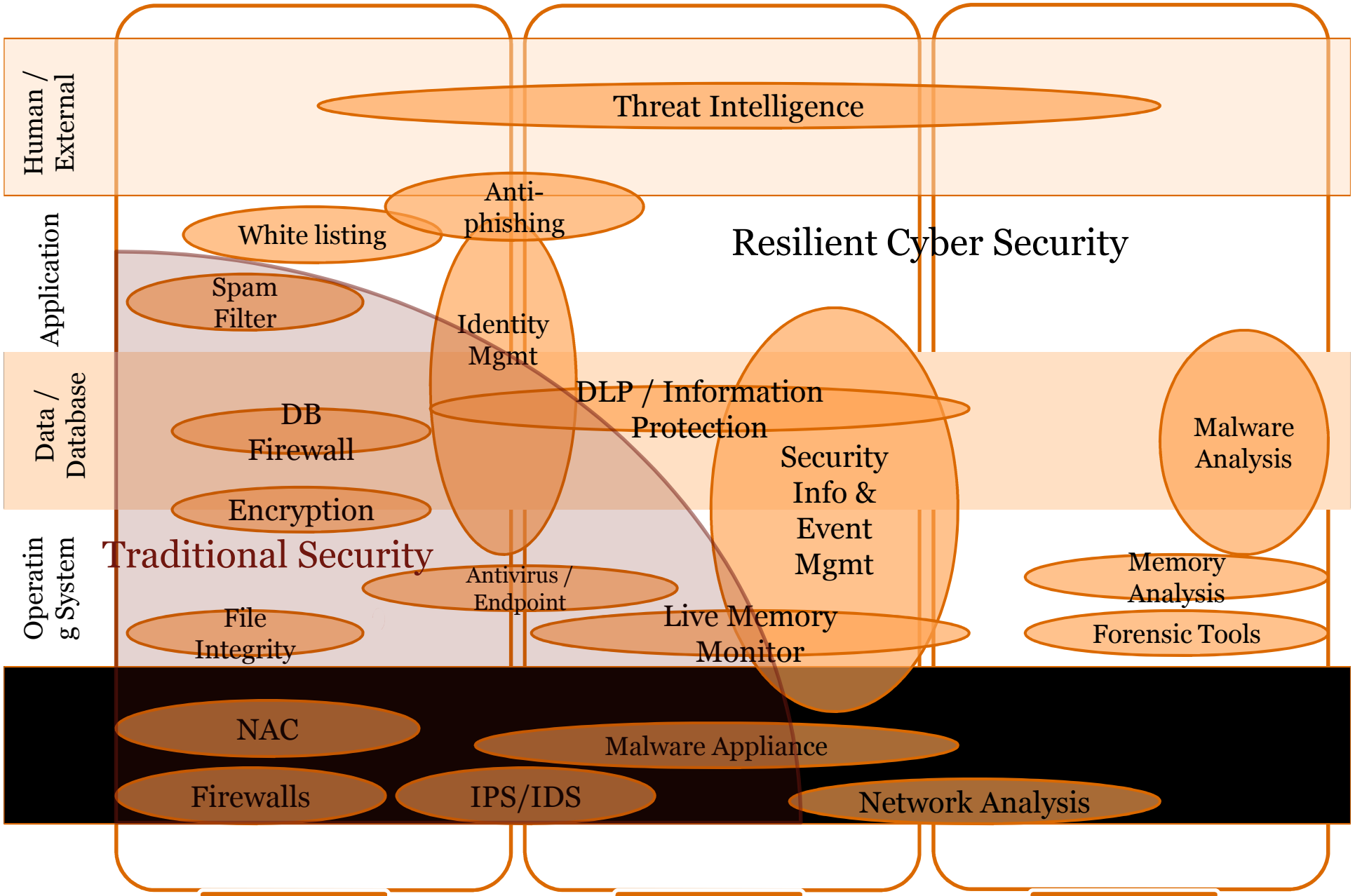
- Investigation costs
- Legal costs
- Brand damage
- State and federal regulatory actions
- Third-party and class action lawsuits
- Business partner lawsuits/indemnification

Why organizations have not kept pace

Years of underinvestment in certain areas has left organizations unable to adequately adapt and respond to dynamic cyber risks.



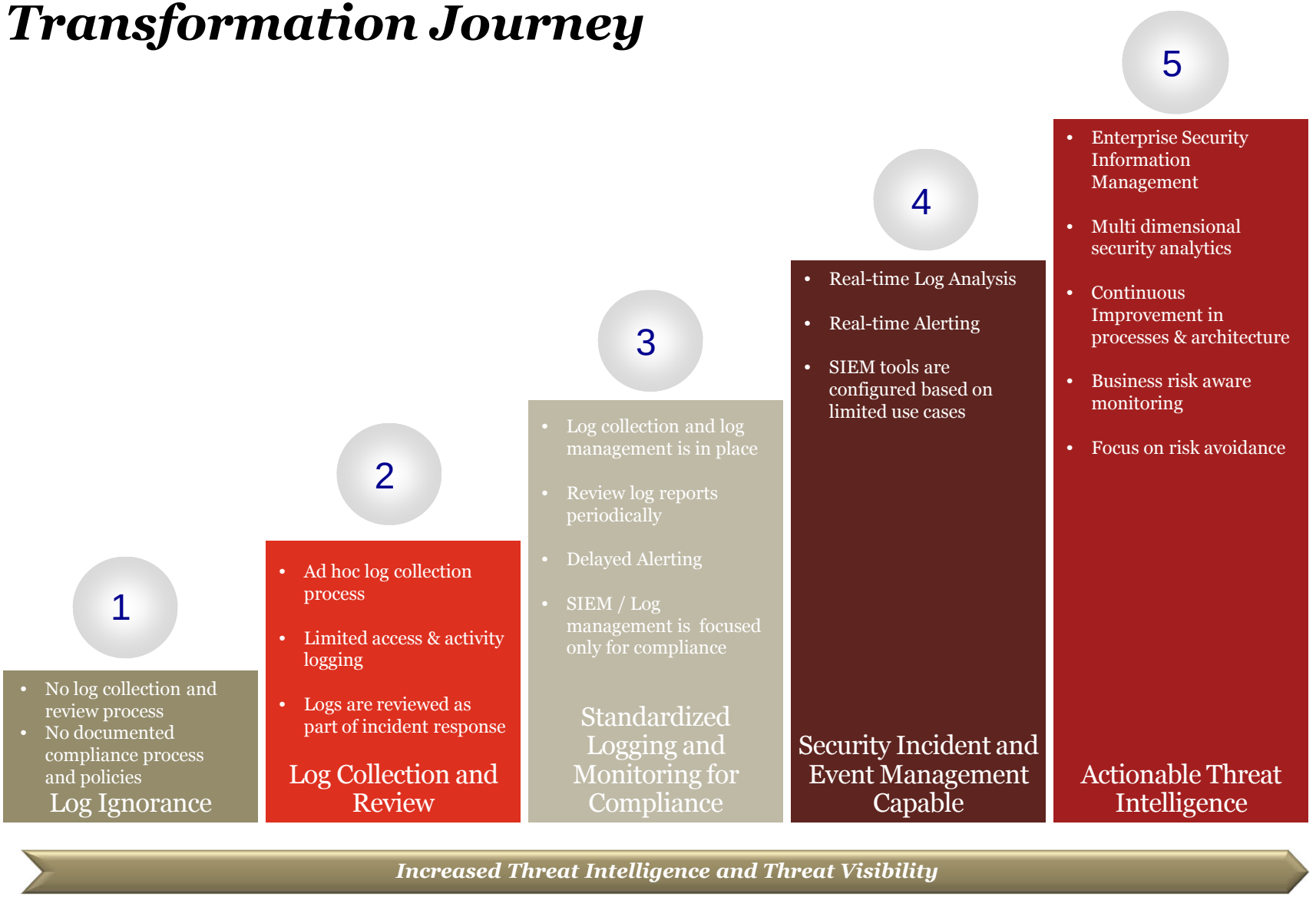
Functional Security Capabilities



Managing the risks

- Know the Who, What, Where of your sensitive data
- Ignoring compliance is not an option
- Review internal policies and procedures
- Update privacy policy
- Make your plan bigger than technology
- Review existing insurance coverage
- Monitor and audit
- Establish call-back procedures to help defend against social engineering
- Consider using encryption
- Control or limit access to payment and other sensitive systems

Transformation Journey



Responding to a breach

Maintain an incident-response plan and team

- Identify team members and responsibilities
- Outline breach response measures
- Involve outside professionals (legal, forensic, public relations)

Consult with legal counsel

- Guide breach response
- Ensure compliance
- Preserve applicable privileges

Preserve digital evidence

- Do not alter compromised systems
- Do not turn compromised machine off; isolate from network
- Preserve logs and log all actions taken

Responding to a breach

Maintain network diagrams and Scan to detect rogues

- Provides quick, clear picture of environment

Establish vendor and law enforcement relationships

Be accurate and be fast

- Prepare to implement a communications plan
- Communicate at the earliest appropriate opportunity
- Commit to updating as more facts become available

Containment

- Prevent further compromise

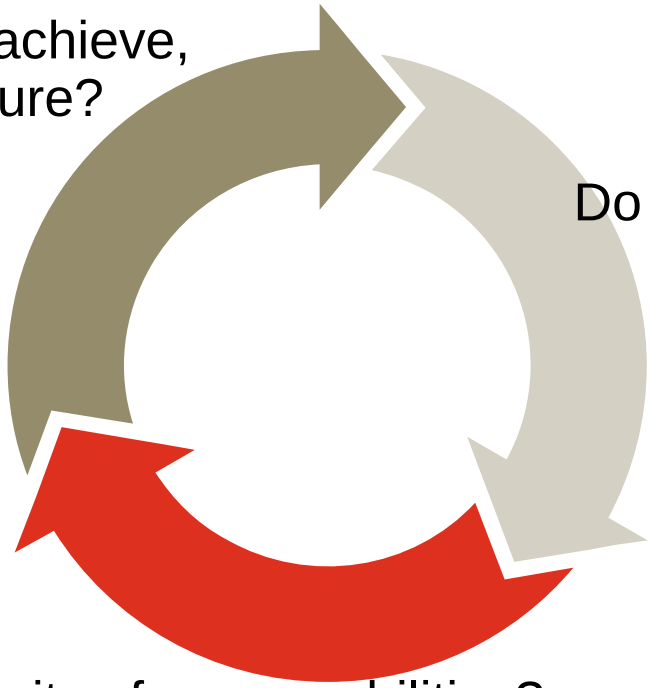
Remediation

- Patch vulnerabilities (ALL vulnerabilities and ALL devices connected to the net)

Given all this, how should Internal Audit (IA) respond to rapidly evolving risks and threats?

Addressing the board level discussion.

What are we trying to achieve, and how do we measure?



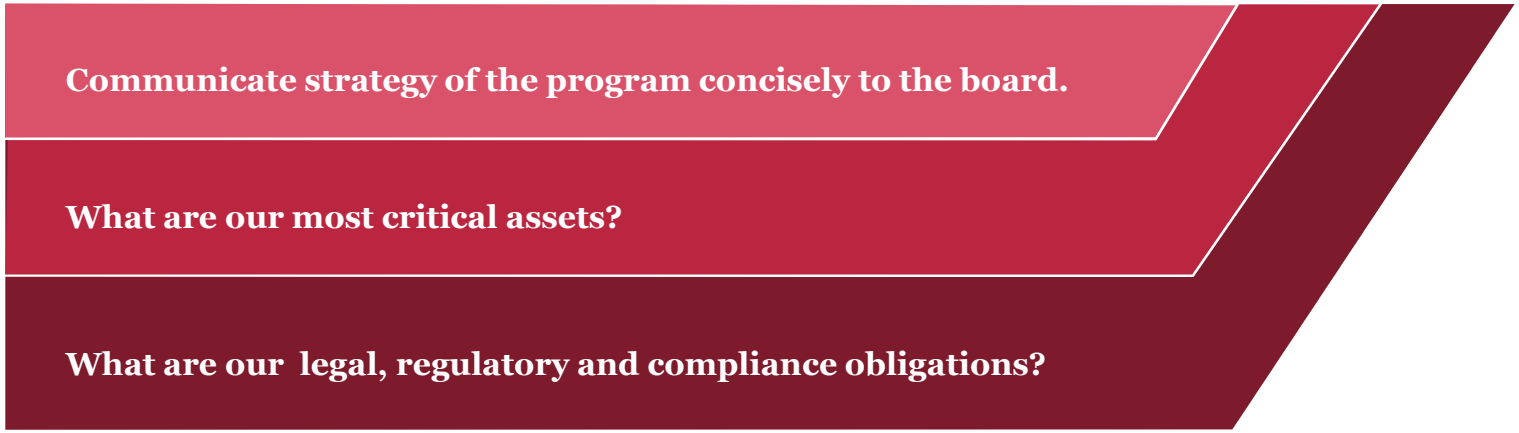
Do we understand our risk?

Do we know the maturity of our capabilities?

Do we understand our risk?

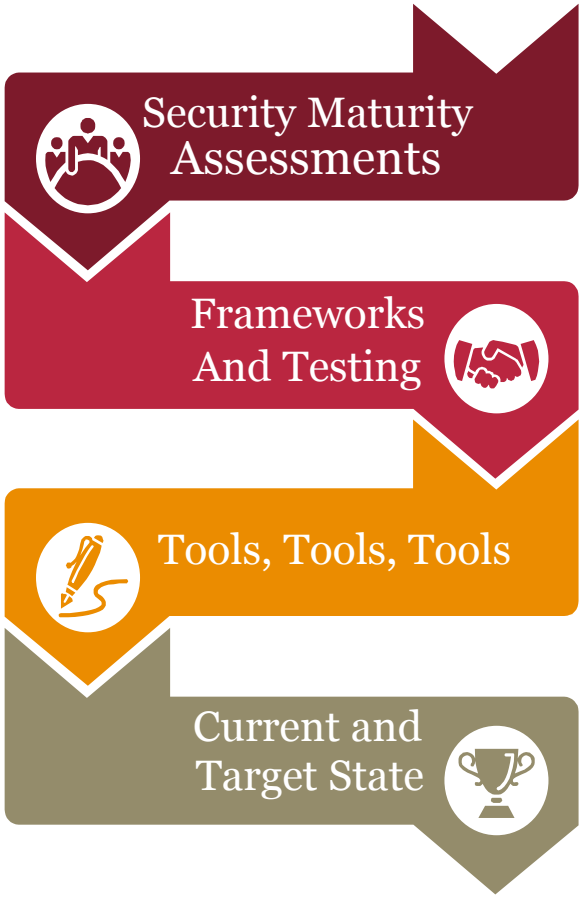
Value

Summarize Risk Simply



Do we know our capabilities?

Traditional risk assessments do not assess whether the information security strategy and program is aligned with the business strategy.



1. Profile the Program
2. Conduct Industry Benchmark
3. Score Program maturity

PwC's ATLAS, NIST CSF, C2M2, FISMA, 800-53, etc.

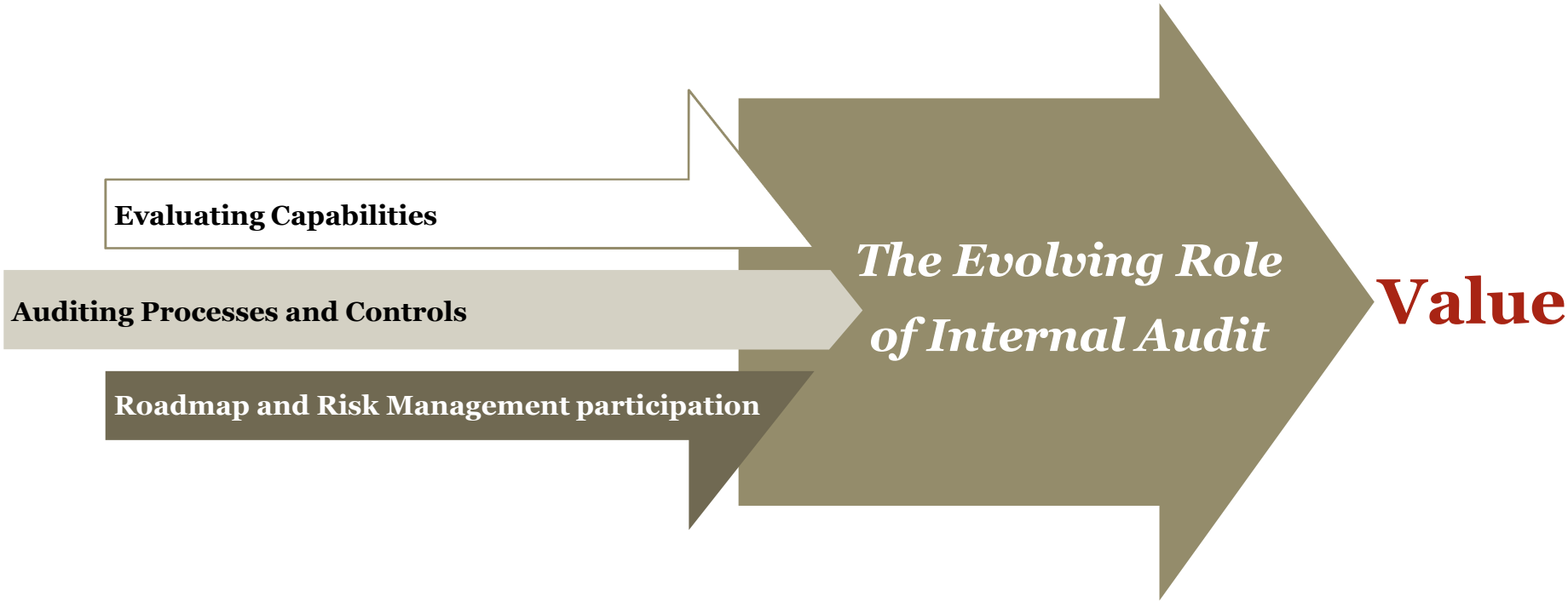
Detail and process testing – both are needed.

Investment in tools does not necessarily mean a capability has been developed.

Where are we?

Where do we want to be?

Evolving role of IA – Measuring achievement and strategic alignment



IA Focus Areas

Threat and Vulnerability Management

- How is cyber intelligence integrated into the vulnerability management program?
- Patch management and system hardening are highly technical yet these capabilities should be understood and evaluated
- Evaluation requires a detailed understanding of your IT architecture

Common pitfalls

- Security by obscurity is no longer relevant with operational technology
- End of life systems are improperly managed
- Asset management does not support vulnerability management
- Metrics are incomplete or not used at all

IA Focus Areas

Governance and IT Risk Management

- Strong security practices develop from mature capabilities, grounded by documented policies and procedures
- A consistent, metrics driven process to substantiate progress with information security initiatives
- Formal IT security risk management to determine how to react when vulnerabilities are detected

Common pitfalls

- Not prioritizing security based on the risk to the organization – where is your sensitive data or valuable assets?

IA can provide value in every one of these activities.

1. Ensure that your cybersecurity strategy is aligned with business objectives and is strategically funded
2. Identify your most valuable information assets, and prioritize protection of this high-value data
3. Understand your adversaries, including their motives, resources, and methods of attack to help reduce the time from detect to respond
4. Assess cybersecurity of third parties and supply chain partners, and ensure they adhere to your security policies and practices
5. Collaborate with others to increase awareness of cybersecurity threats and response tactics

For more information on cybersecurity…

www.pwc.com/cybersecurity

- Results of 2015 Global State of Information Security
- Answering you cybersecurity questions; the need continued action
- 2013 US State of Cybercrime Survey Whitepaper
- 10Minutes on the stark realities of cybersecurity
- Cybersecurity risk on the board's agenda
- Cyber Video Series
- A response to the President's Cybersecurity Executive Order

Key Contacts

Richard Dorough
Managing Director
Ft. Worth, TX
richard.e.dorough@us.pwc.com
(817) 296-2835

Ashley Shugart
Manager
Dallas, TX
ashugart@us.pwc.com
(202) 679-5939

Matthew Wilson
Director
Dallas, TX
matthew.l.wilson@us.pwc.com
(678) 427-1042