Cybersecurity Update for Internal Auditors

Matt Wilson, PwC Risk Assurance Director

pwc

Introduction and agenda

- Themes from The Global State of Information Security® Survey 2014
- The enterprise cyber security challenge
- How internal auditors can respond
- Tools at your disposal – NIST cyber security framework and security maturity models
- Security capability considerations for internal auditors

The Global State of Information Security® Survey 2014

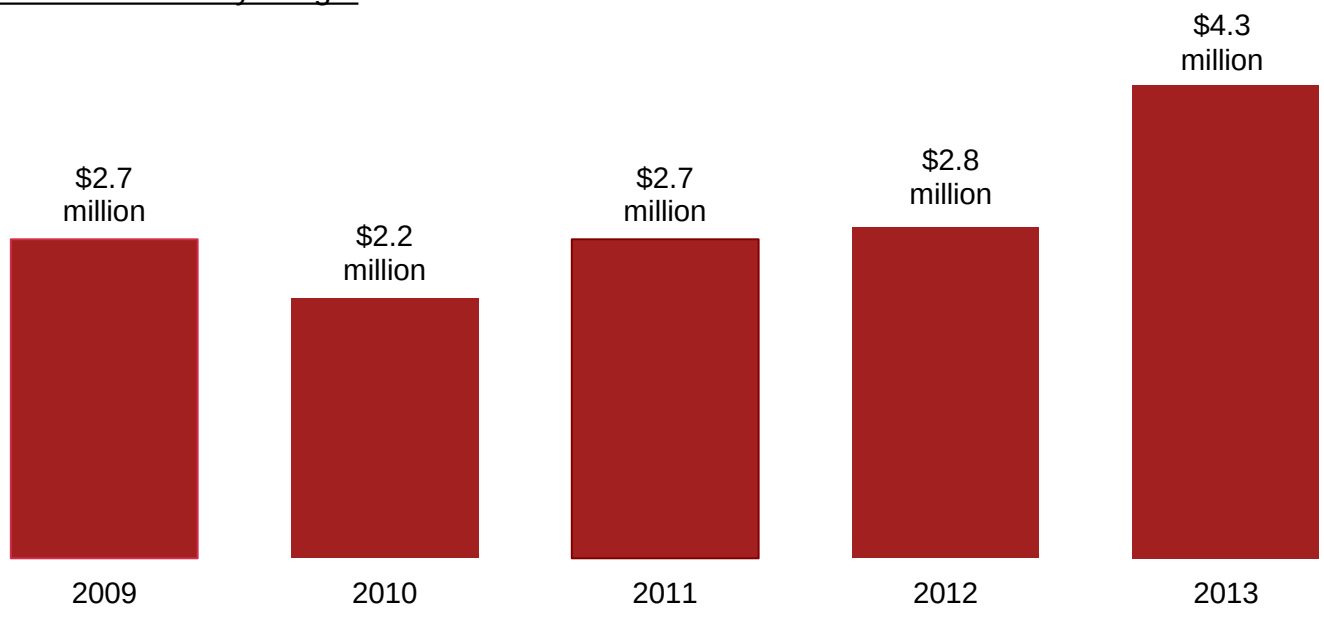
- Worldwide study by PwC, CIO magazine, and CSO magazine
- PwC's 16th year conducting the online survey, 11th with CIO and CSO magazines
- More than 9,600 responses from executives including CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security

Number of responses this year	
Technology	1,226
Financial Services	993
Retail & Consumer	820
Public Sector	694
Industrial Products	671
Telecommunications	456
Healthcare Providers	398
Entertainment & Media	221
Automotive	209
Aerospace & Defense	193
Power & Utilities	143
Oil & Gas	107
Pharmaceutical	74

Information security budgets increase significantly

Security budgets average $4.3 million this year, a gain of 51% over 2012. Organizations understand that today's elevated threat landscape demands a substantial boost in security investment.

Average information security budget

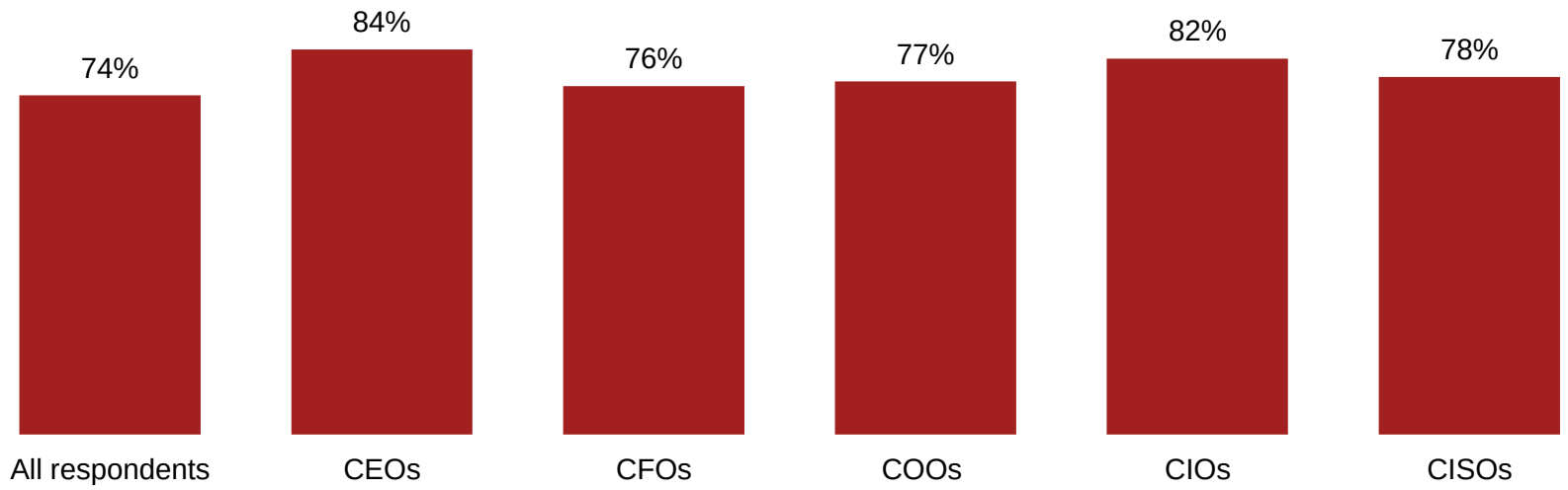


Question 8: "What is your organization's total information security budget for 2013?"

Confidence is high: 74% of respondents believe their security activities are effective, with top execs even more optimistic

In the C-suite,* 84% of CEOs say they are confident in their security program. Note that CFOs are the least confident among executives.

Executive confidence in effectiveness of security activities (somewhat or very confident)

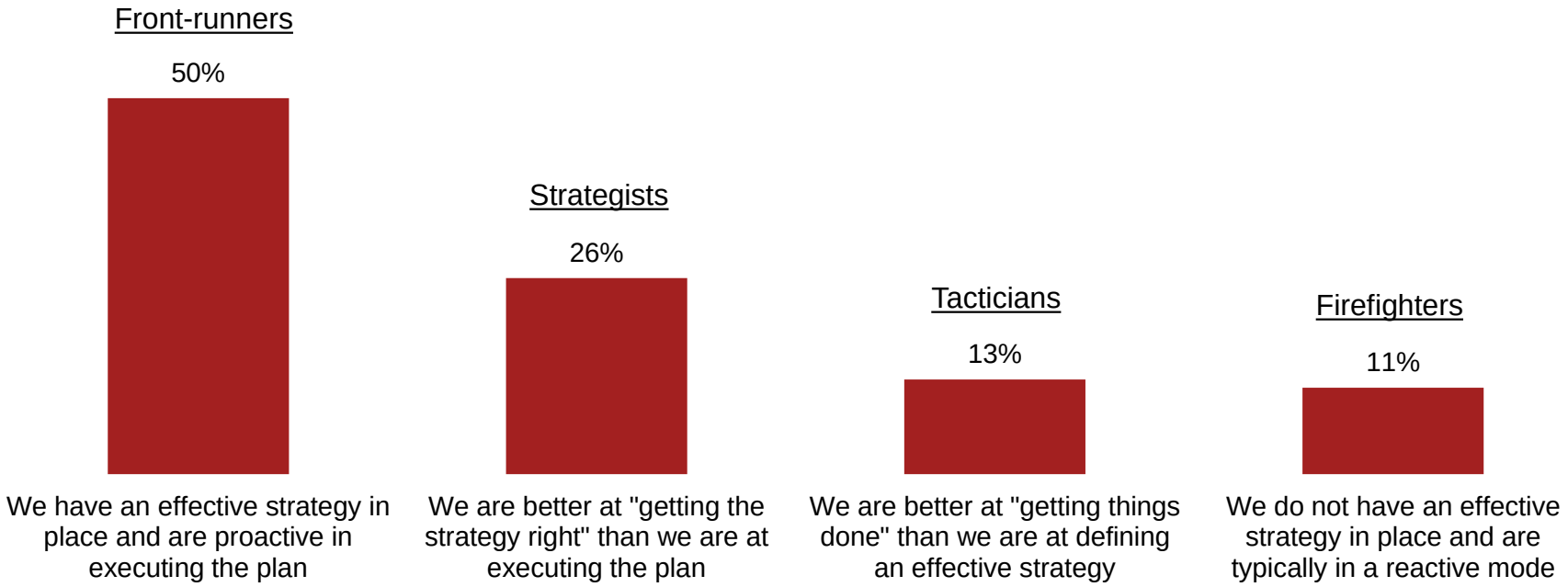


* CEOs, CFOs, and COOs

Question 39: “How confident are you that your organization’s information security activities are effective?” (Respondents who answered “Somewhat confident” or “Very confident.”) Question 1: “My job title most closely resembles”

Half of respondents consider themselves "front-runners," ahead of the pack in strategy and security practices

50% say they have an effective strategy in place and are proactive in executing the plan, a 17% increase over last year. About one in four (26%) say they are better at getting the strategy right than executing the plan.



Question 27: "Which statement best characterizes your organization's approach to protecting information security?"

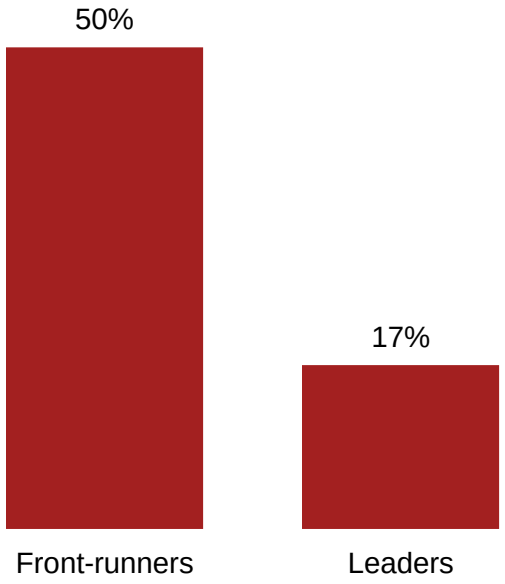
But closer scrutiny reveals far fewer real leaders than front-runners

We measured respondents' self-appraisal against four key criteria to filter for leadership.

To qualify, organizations must:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year

Our analysis shows there are still significantly fewer real leaders than self-identified front-runners.

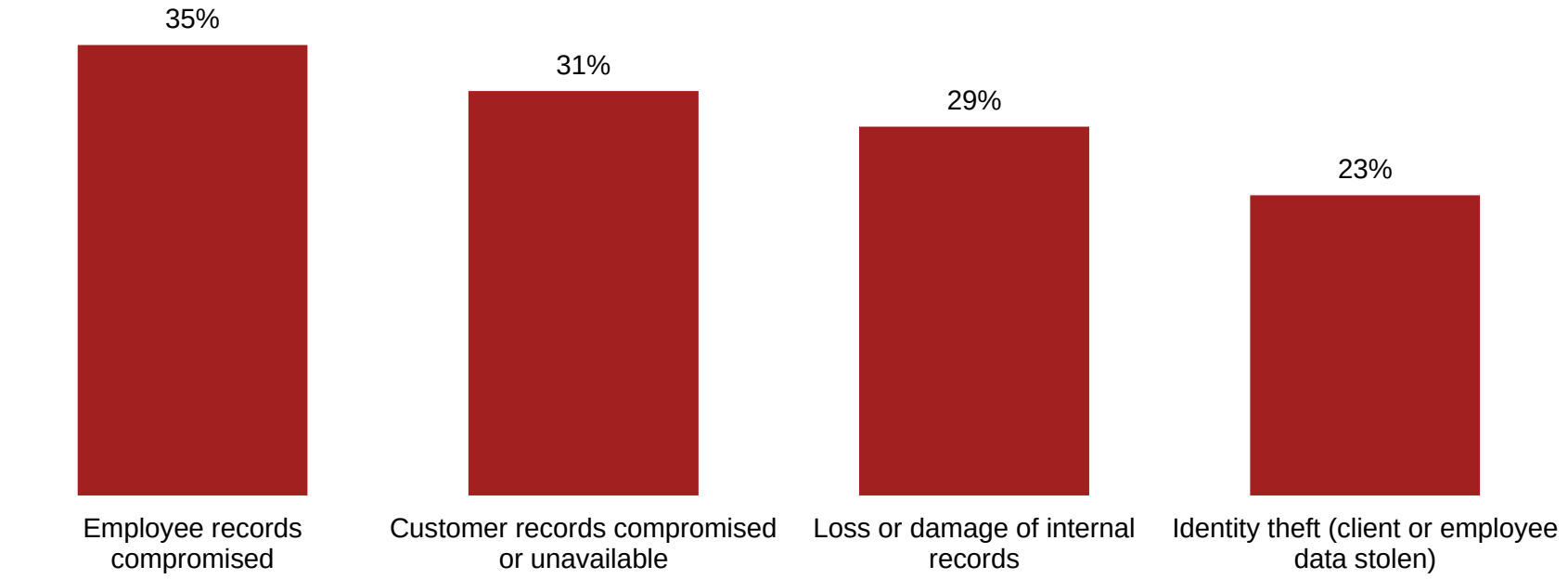


Leaders are identified by responses to Question 13A: "Where / to whom does your CISO, CSO, or equivalent senior information security executive report?" Question 14: "What process information security safeguards does your organization currently have in place?" Question 19: "What types of security incident(s) occurred?" Question 31: "Over the past year, has your company measured and reviewed the effectiveness of its information security policies and procedures?"

Employee and customer data continue to be easy targets

Compromise of employee and customer records remain the most cited impacts, potentially jeopardizing an organization's most valuable relationships. Also significant: Loss or damage of internal records jumped more than 100% over last year.

Impact of security incidents

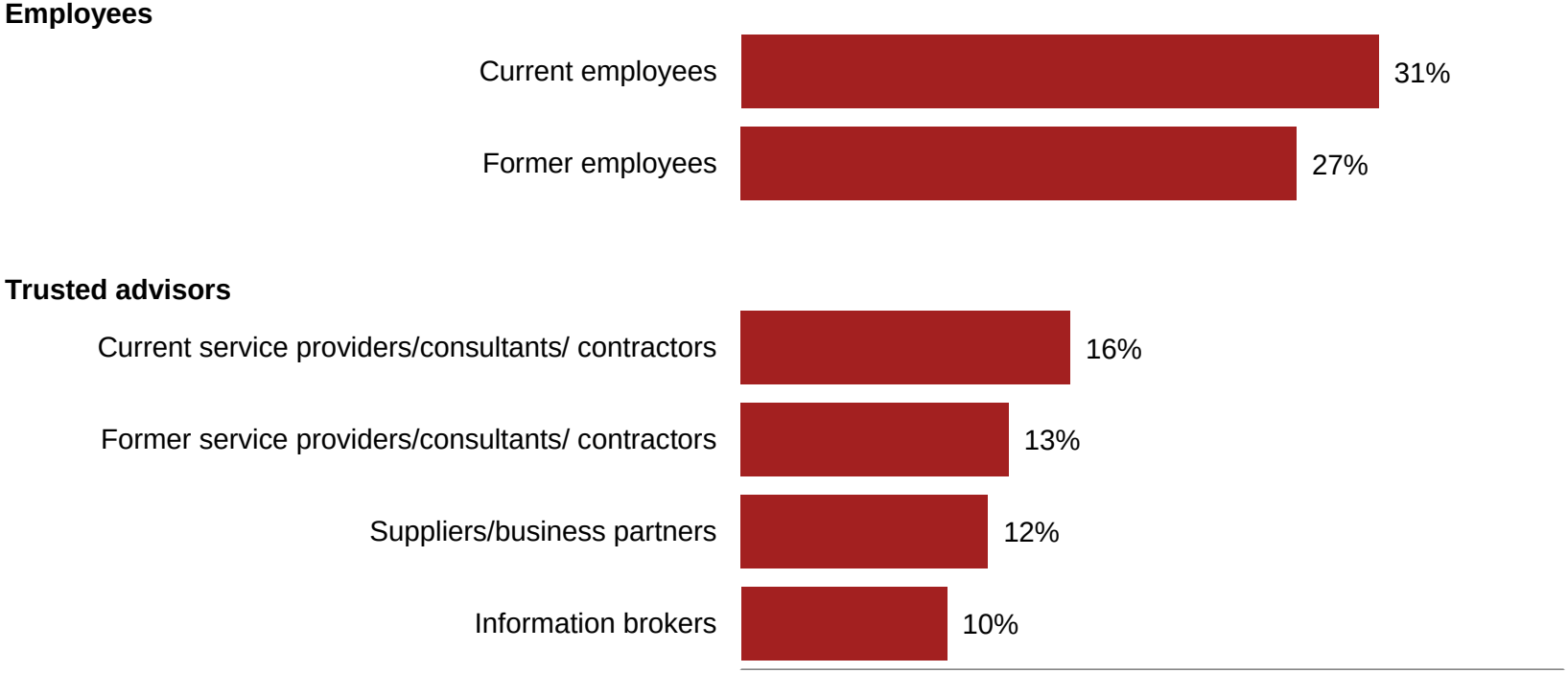


Question 22: "How was your organization impacted by the security incidents?" (Not all factors shown.)

Insiders, particularly current or former employees, are cited as a source of security incidents by most respondents

It's the people you know—current or former employees, as well as other insiders—who are most likely to perpetrate security incidents.

Estimated likely source of incidents

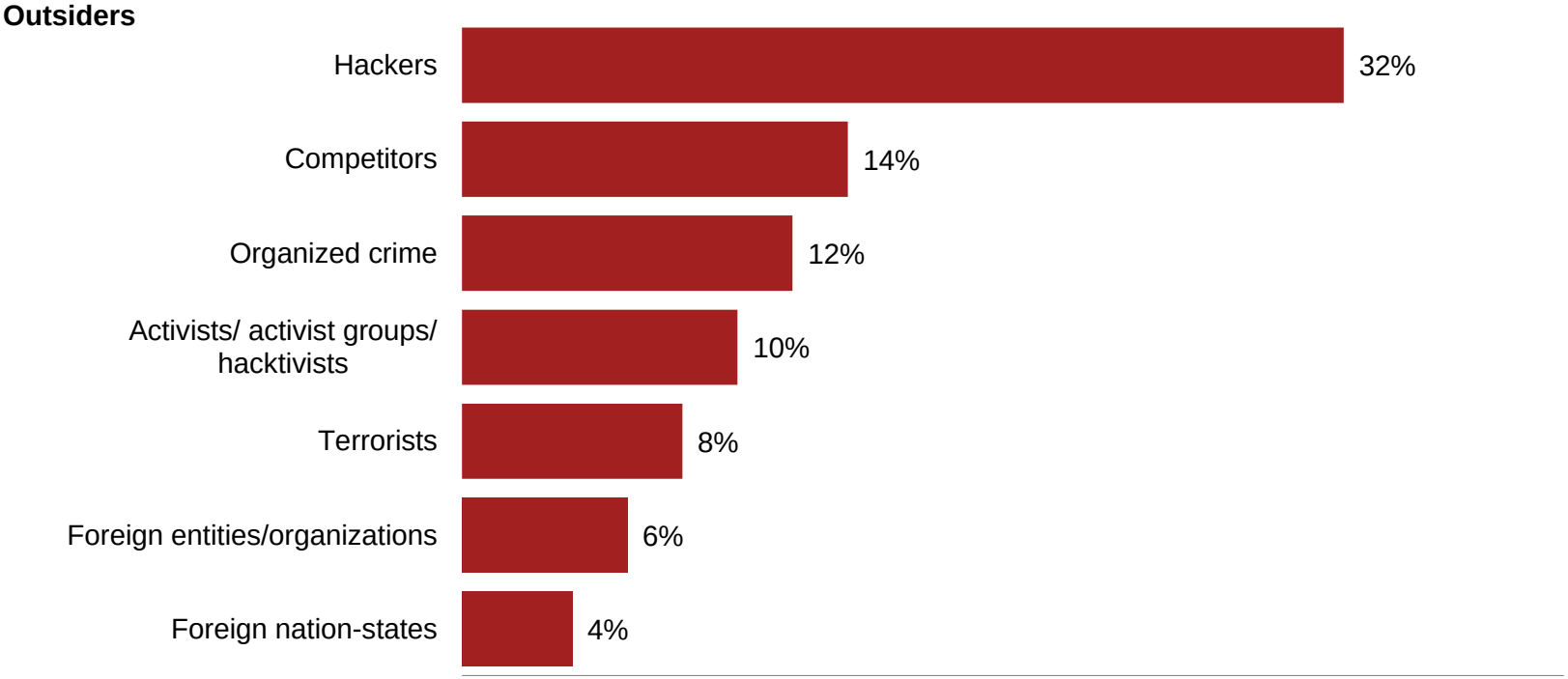


Question 21: "Estimated likely source of incidents" (Not all factors shown.)

While attacks backed by nation-states make headlines, your organization is more likely to be hit by other outsiders

Only 4% of respondents report security incidents perpetrated by foreign nation-states. Hackers represent a much more likely danger.

Estimated likely source of incidents



Question 21: “Estimated likely source of incidents” (Not all factors shown.)

The enterprise cybersecurity challenge

- CEOs, board members, and business executives should understand that security risks are organizational threats
- It is an enterprise-wide issue that suffers from significant knowledge gaps
- Compliance is different from security

The enterprise cybersecurity challenge

- Risk acceptance decisions are generally not well communicated
- Investment is challenging to justify because impact is challenging to predict
- Evaluation methods generally focus on measuring a sample of the output
- All this results in poor self awareness – have we mitigated enough risk?

How internal auditors can respond

- Evaluate security strategy based on the organization's knowledge of threats, assets and adversaries
- Assess your company's capabilities around security governance, security operations, and incident response
- Re-think your typical process and controls based approach – it is typically focused on one area of risk (e.g., patch management), rather than the broader capability (e.g., threat identification and mitigation)

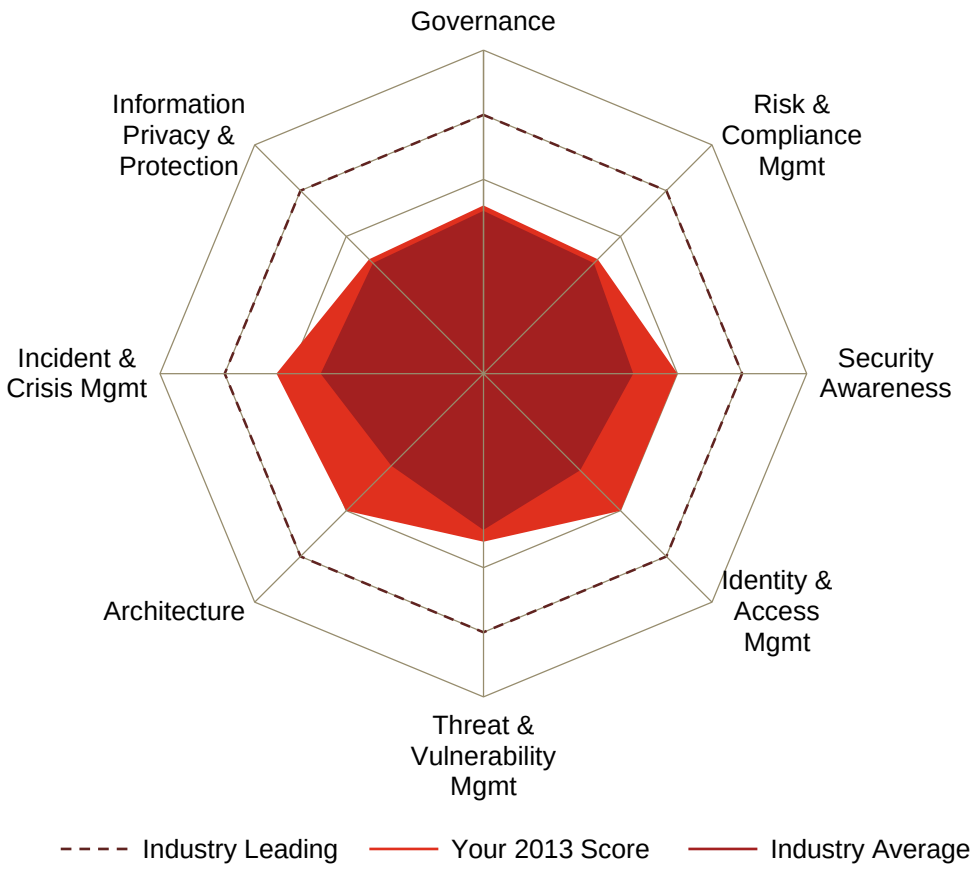
How internal auditors can respond

- Remain skeptical and promote self awareness
- Identify where risk acceptance is poorly communicated
- Help communicate that capability growth is necessary to keep up with the changing threats
- The CAE plays an important role in conversation with senior management and the board

Executive Order 13636 – NIST Cybersecurity Framework

- A framework to assist organizations responsible for critical infrastructure to manage cybersecurity risk – scheduled to be finalized in February 2014
- Future legislation could point to this framework as a way to suggest meeting requirements – Congress will monitor adoption rates for the framework
- Not a control framework – instead, provides a common language and mechanism for organizations to:
    1. Describe their current cybersecurity posture;
    2. Describe their target state for cybersecurity;
    3. Identify and prioritize opportunities for improvement within the context of risk management;
    4. Assess progress toward the target state; and,
    5. Foster communications among internal and external stakeholders.

Maturity model approach to measure information security capability



Baseline helps to:

- Communicate the design and value of your cyber security program to senior management and the board of directors
- Validate that your cyber security investments are resulting in reducing your (overall) vulnerability footprint
- Justify security improvements and/or investments
- Prioritize security initiatives
- Measure year-over-year progress
- Focus IT audit resources on areas of higher risk and change

Security capability considerations – Program Governance

- 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?

Security capability considerations – 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

Security capability considerations – Incident Response

- Assume your adversaries have access – they do
- Response plans need to be documented, communicated and simulated
- The business needs to be prepared – who is involved, e.g., legal?

Common pitfalls

- Monitoring and response capabilities are typically siloed
- Our team is experienced and will react in the event of a cyber attack, we don't need to document or practice it

Security capability considerations – Training and Awareness

- Advanced attacks take advantage of the most vulnerable resources, your people
- Consider the technology that is in place to enable your organization to practice good security
- Best programs make it relevant to the individual

Security capability considerations – Technical Tools

- Firewalls, VPNs, IDS/IPS and Antivirus are standard architecture elements
- What is your organization using to monitor for advanced persistent threats?
  - Organized, targeted, multi-facet, camouflaged attacks
  - Advanced malware detection
  - Advanced elements include: Security Information and Event Management (SIEM), Data Loss Prevention (DLP)

Common pitfalls

- Investment in tools does not necessarily mean a capability has been developed
  - Training, clear roles and responsibilities, time, and management support/monitoring

Security capability considerations – Penetration Testing

Benefits

- Brings experienced professionals to assess weaknesses in your IT architecture footprint
- Helps prioritize vulnerability remediation to areas of high risk
- Provides evidence of exploitation, a powerful communication tool

Limitations

- Point-in-time assessment
- Challenging to interpret
- Focused on the path of least resistance
- Does not simulate an advanced persistent threat
- Does not replace vulnerability analysis
- Does not consider governance or risk management

Internal auditors should remember…

- Cyber security capabilities need to be understood in the context of how the organization can identify, protect, respond, and recover from a cyber event
- Tools are at your disposal, and should be used in combination to develop a thorough point of view:
  - Cyber security frameworks
  - Capability maturity models
  - Process and controls audits
  - Penetration and vulnerability testing

www.pwc.com