



*cutting through complexity*

# KPMG's 2015 Global Audit Committee Survey

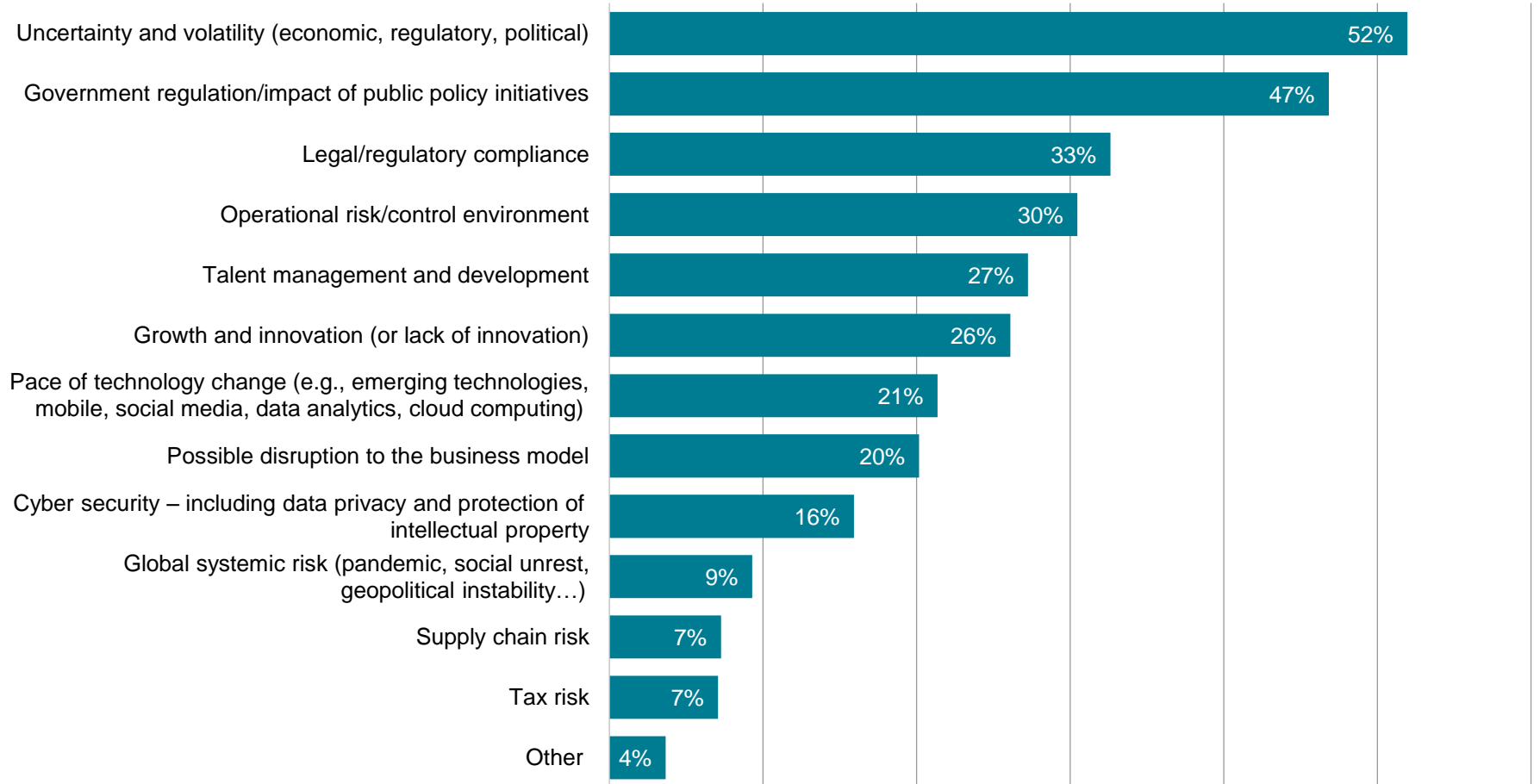
KPMG's Audit Committee Institute

# About KPMG's 2015 Global Audit Committee Survey

- Survey conducted from July – September, 2014
- 1,558 survey responses
- 36 countries represented
- Survey population: audit committee members (or equivalent role)

*May not equal 100% due to rounding*

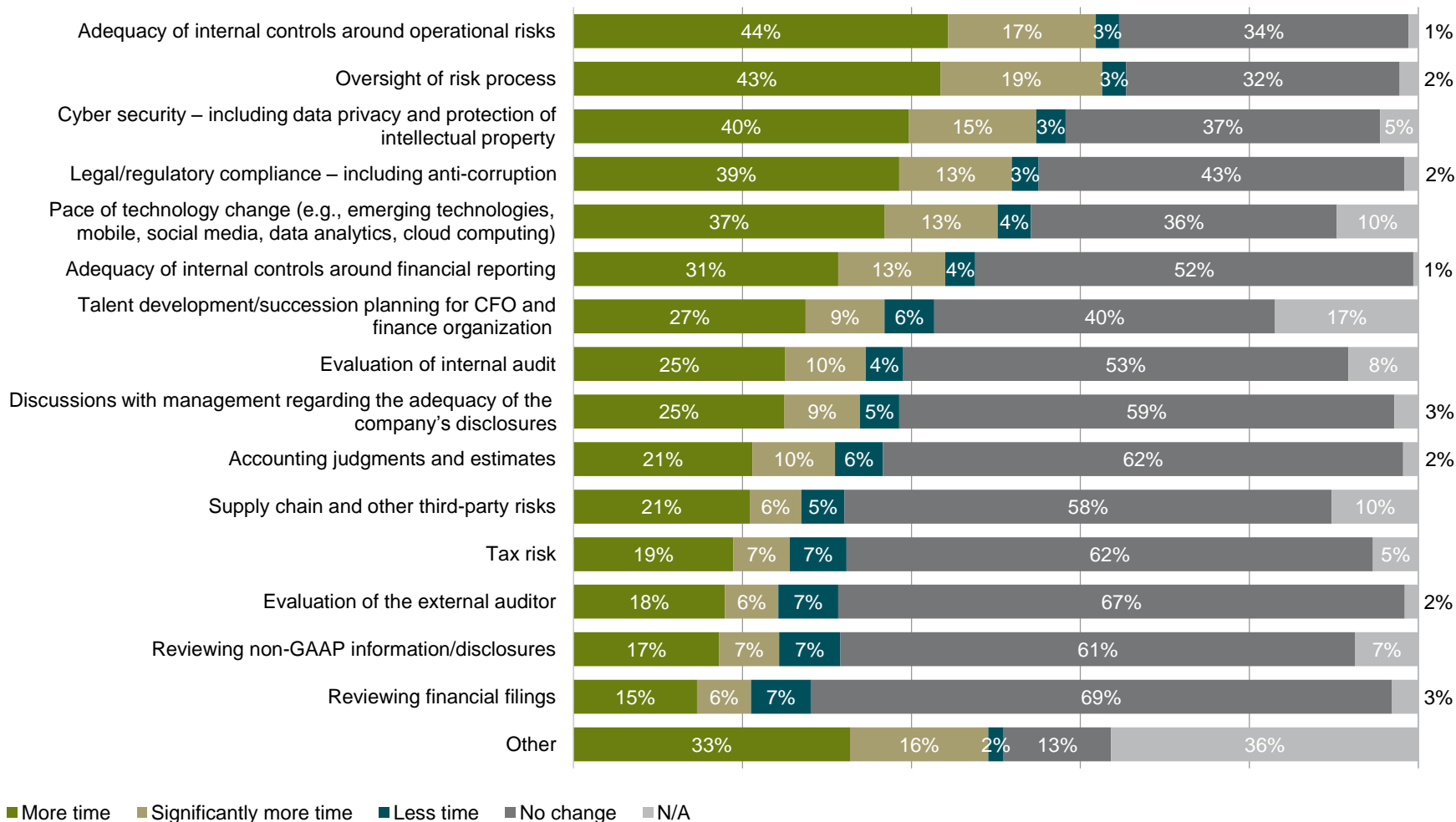
# Q1. Which of the following risks (aside from financial reporting risk) pose the greatest challenges for your company? (Select three)



Multiple Responses Allowed

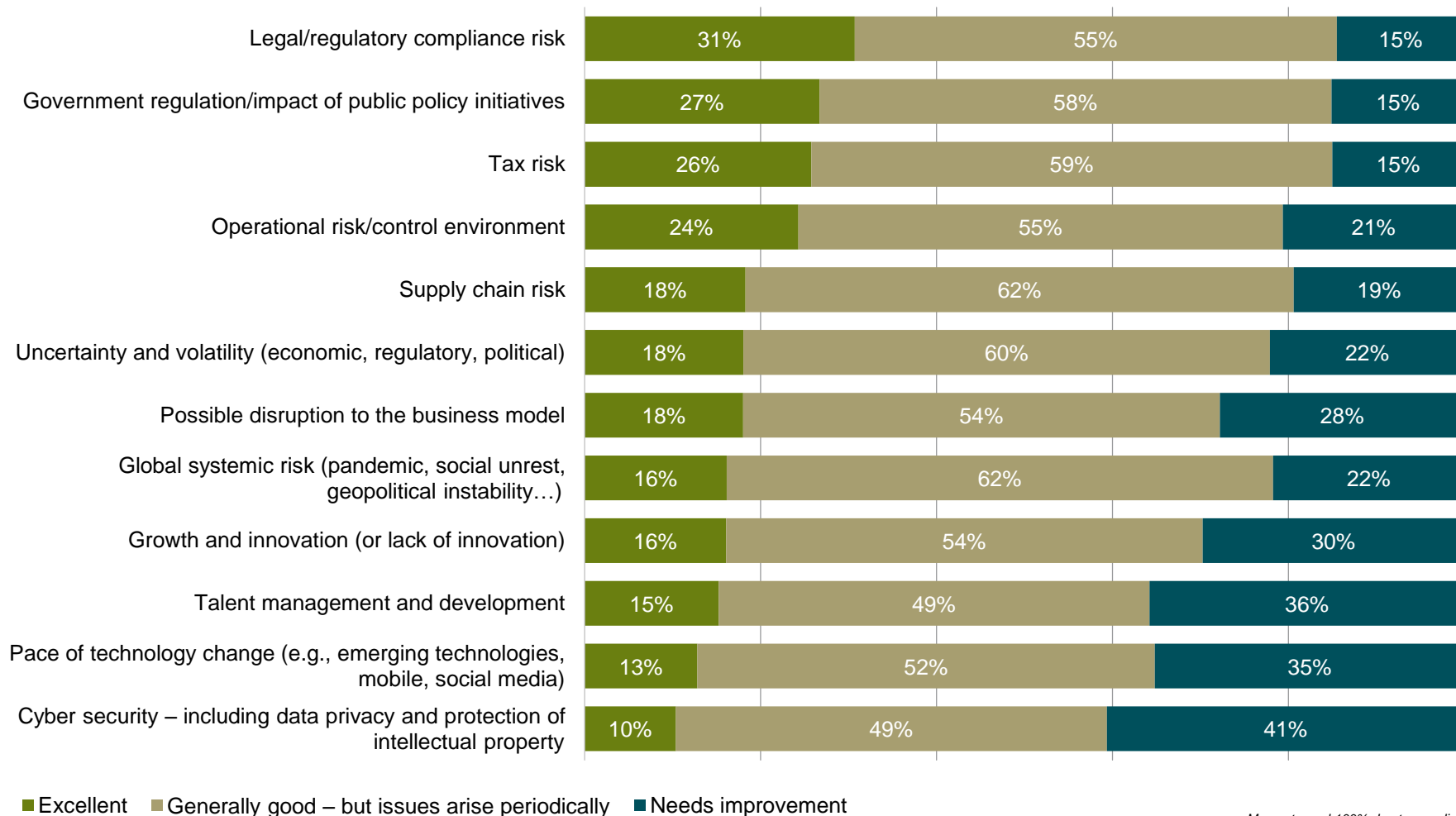


## Q2. How much agenda time should your audit committee devote to the following matters in 2015, compared to 2014? (Note: If the matter is not an audit committee responsibility, please indicate N/A)



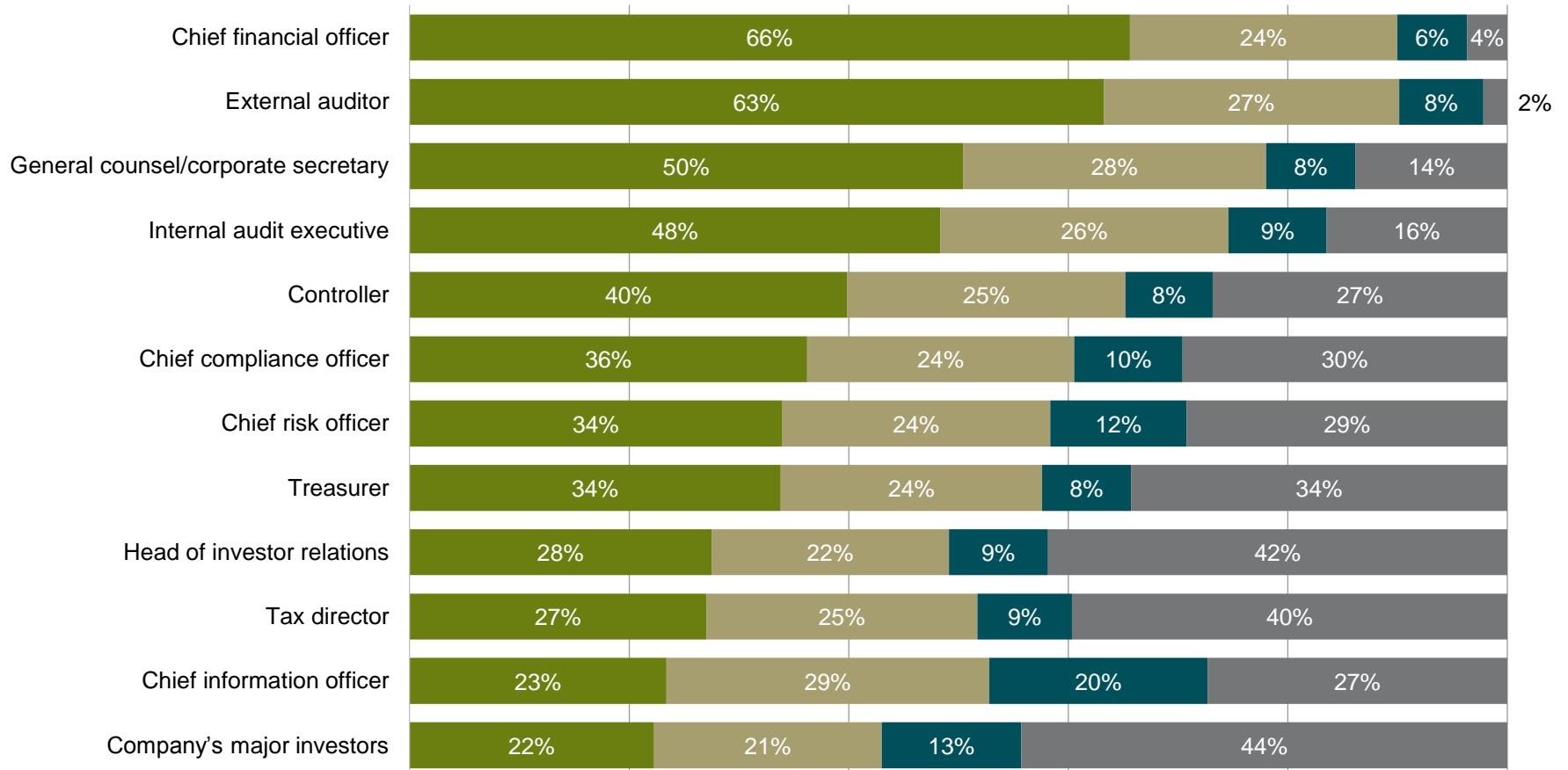
May not equal 100% due to rounding

### Q3. “Please rate the quality of the information you receive – whether as a member of the audit committee, other committee, or full board – about the following risks and their potential impact on the company: Quality of the information is...”



May not equal 100% due to rounding

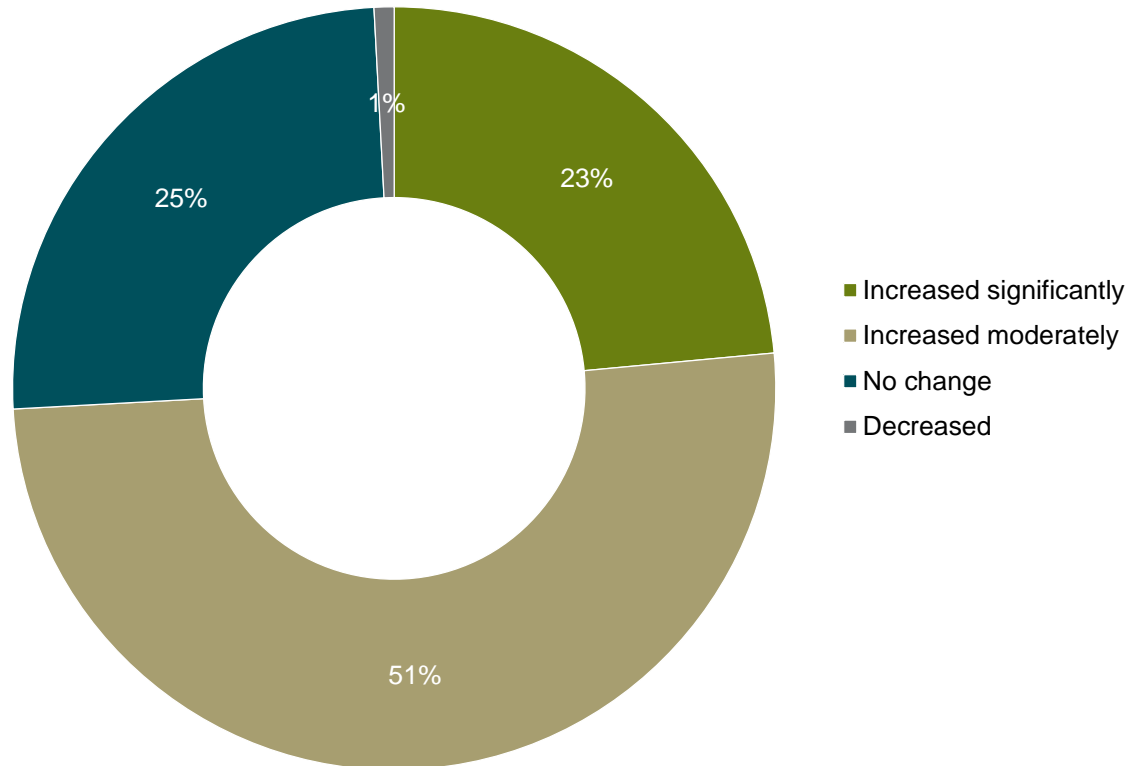
## Q4. Please rate the quality of the audit committee's communications and interactions with the following professionals/functions (or equivalent):



■ Excellent 
 ■ Good, but issues arise periodically 
 ■ Needs improvement 
 ■ N/A or no significant interaction

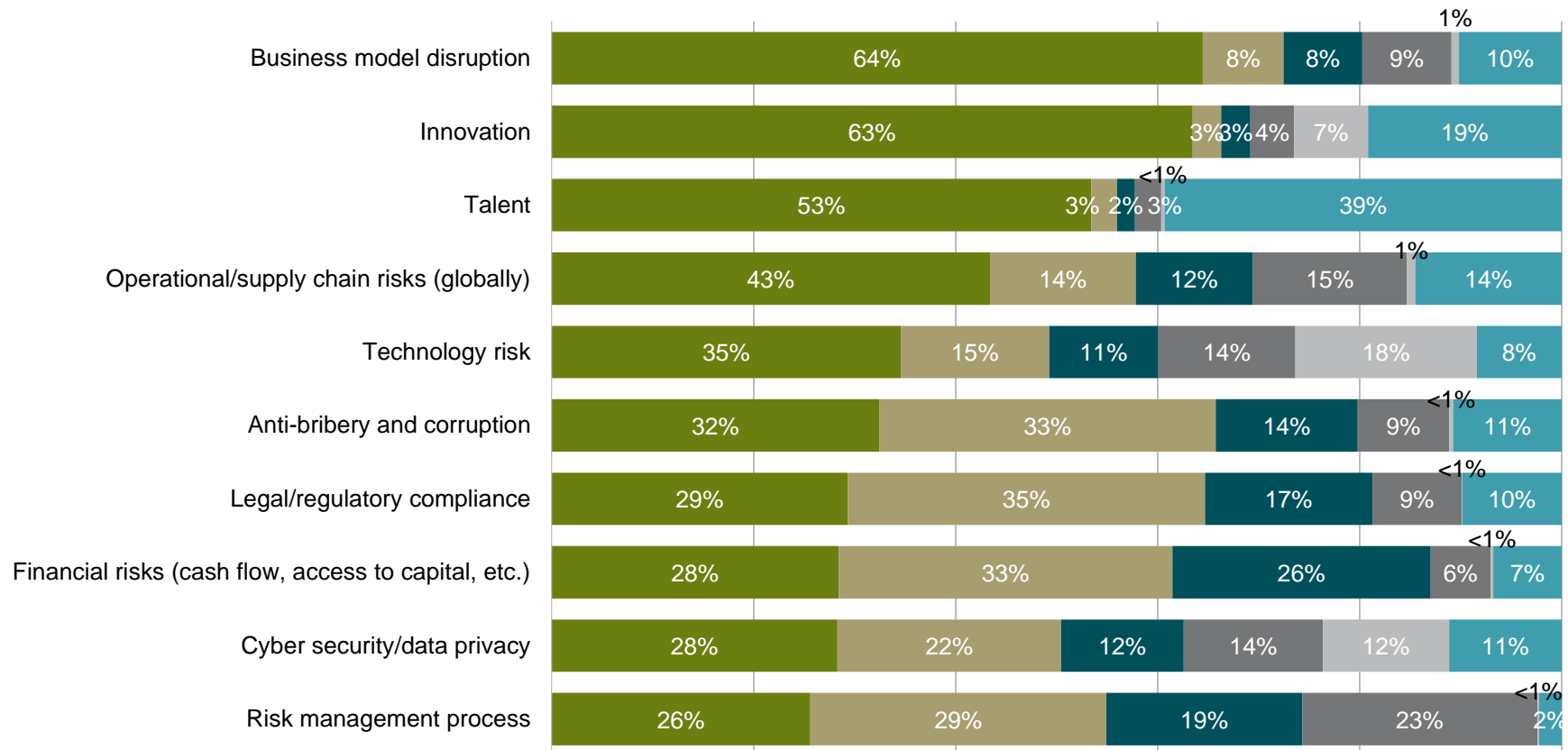
*May not equal 100% due to rounding*

## Q7. To what extent has the amount of time required to carry out your audit committee responsibilities changed over the past two years?



*May not equal 100% due to rounding*

# Q9. To which group has the board assigned the *majority of tasks* directly related to the oversight of the following areas of risk?

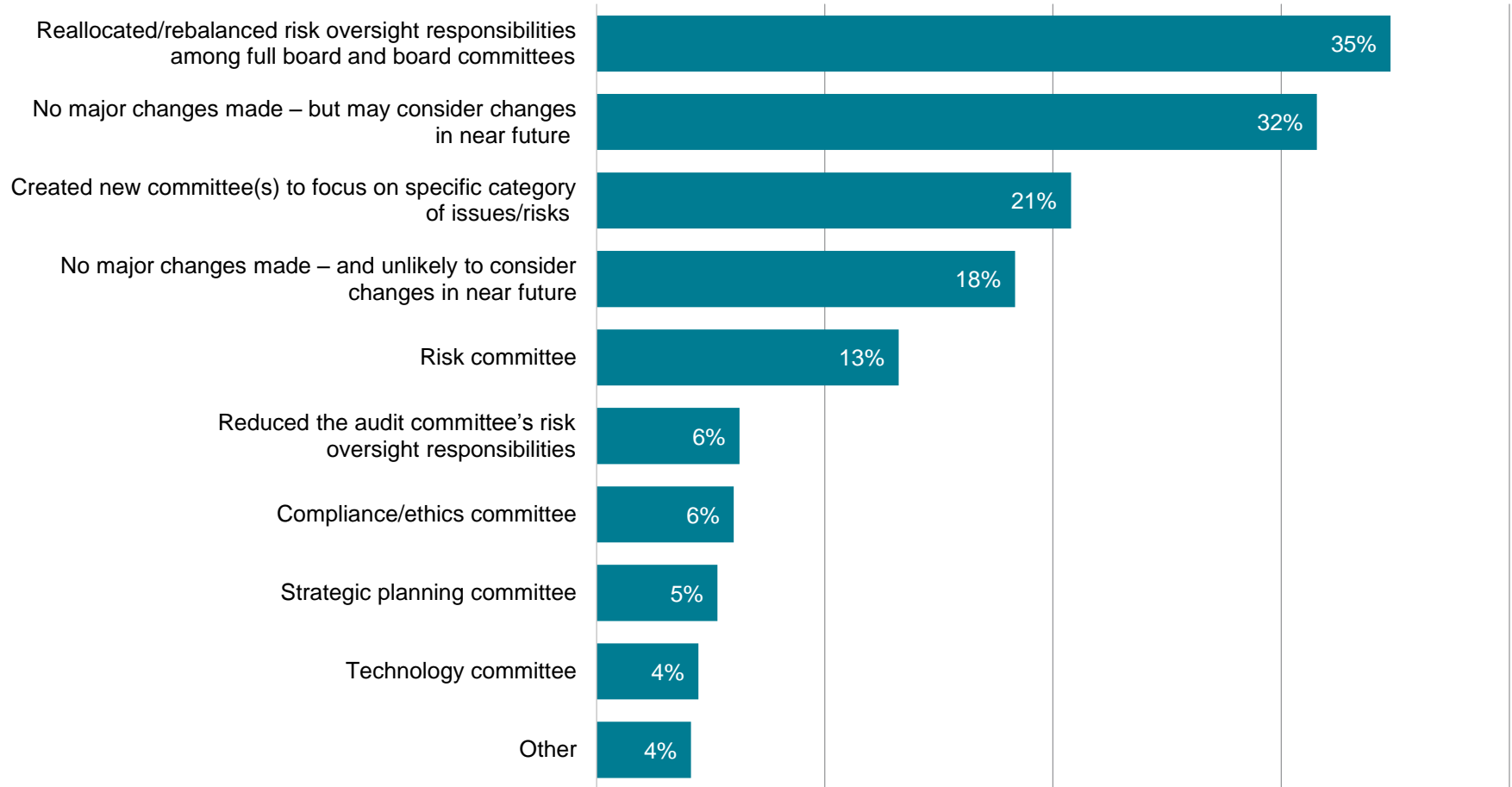


- Full Board
- Audit Committee
- Audit & Risk or Finance Committee
- Risk Committee
- Technology Committee
- Other Committee

May not equal 100% due to rounding

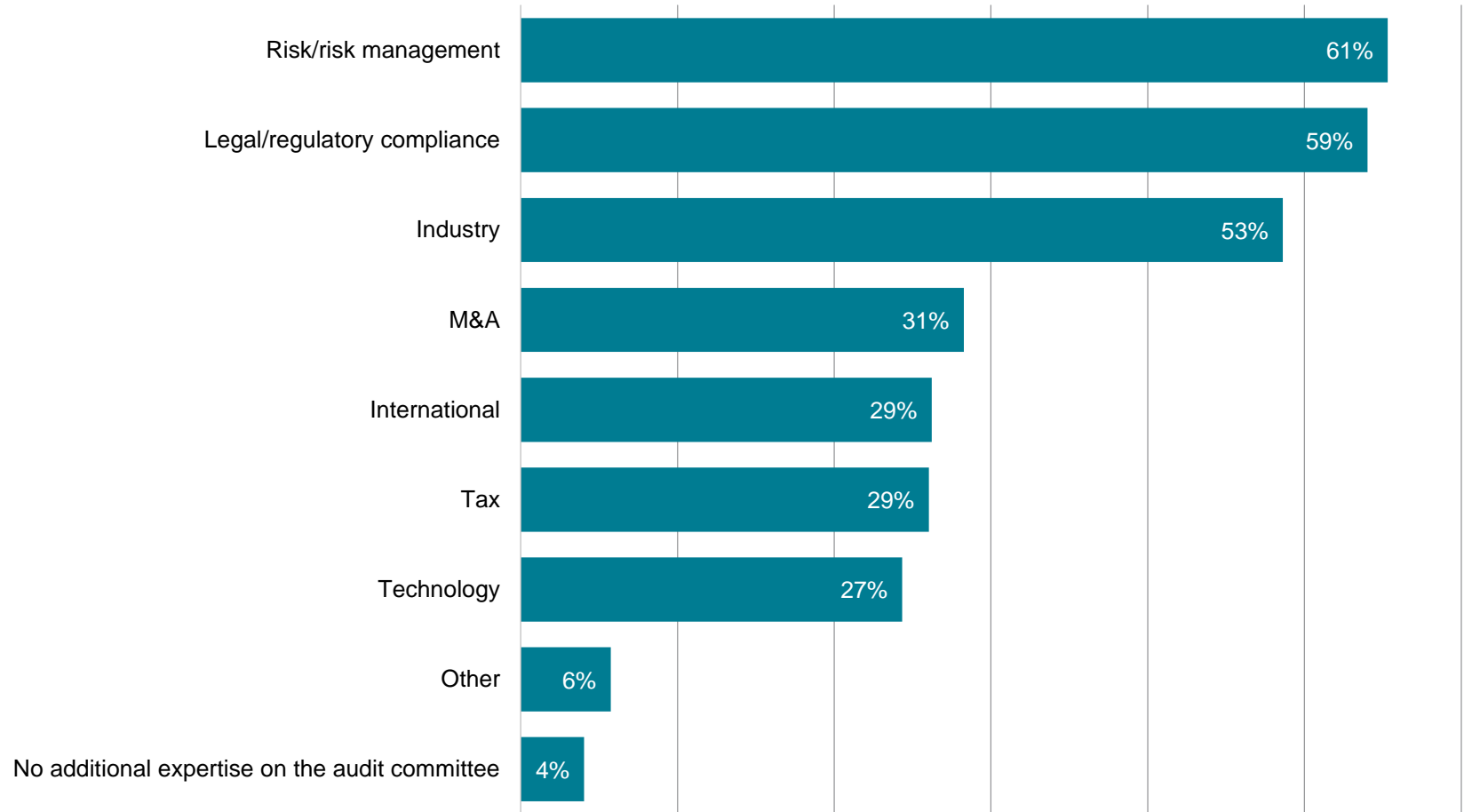


## Q10. In what way has your audit committee's role in risk oversight changed over the past several years? (Select all that apply)



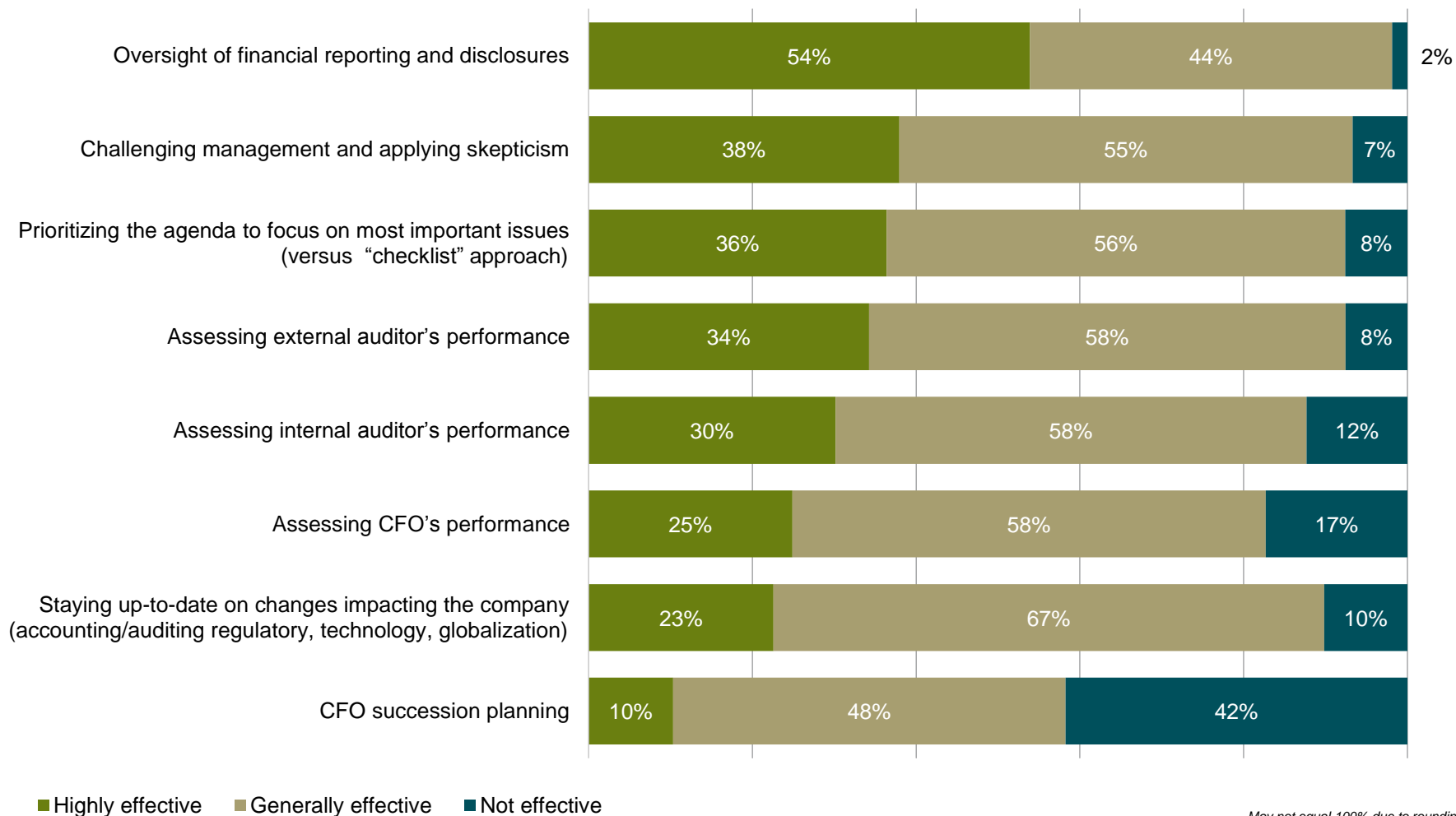
Multiple Responses Allowed

# Q11. In addition to the requisite financial expertise, what other in-depth experience or expertise currently resides on your audit committee? (Select all that apply)



Multiple Responses Allowed

# Q19. Please rate your audit committee's oversight effectiveness in the following areas:



May not equal 100% due to rounding

## Q20. What would most improve your audit committee's overall effectiveness? (Select three)



Multiple Responses Allowed





*cutting through complexity*

# Top Challenges and concerns





# Top Challenges and Concerns

- **Uncertainty and volatility**
  - Speed of change in business and technology / operational risk / regulation and compliance.
- **Risk Oversight**
  - AC's want to spend more time on overseeing risk management processes, operational risk management and cyber / tech risk.
- **Quality of information**
- - Generally good, but needs to improve in areas related to technology and cyber, talent management and innovation. Communication with CIO is seen as poor.
- **Responsibilities**
  - 75% say their workload has increased and the role is getting increasingly difficult. Reallocating responsibilities back to main board or a separate risk committee is a growing trend.

# Top Challenges and Concerns

- **CFO Succession planning**
  - CFO turnover is a concern, along with a lack of visibility into the finance organisation's work (FRM, tax strategy, capital utilization, etc.)
- **Audit Reform and audit quality**
  - Audit quality generally good, confusion about EU audit reform and link to quality, need more insights from auditors and benchmarking.
- **Audit Committee effectiveness**
  - Generally good, but need a better understanding of the business, greater diversity of thinking, open dialogue, broader skillset and more white space.



*cutting through complexity*

# Risk Management Effectiveness and Cyber Security

Thomas Kelly, Partner

Christopher Eaton, Senior Manager, IT Advisory

May 6, 2015

# Introduction

- Globally companies and their boards will continue to deal with a difficult trading environment. Many challenges will be similar, but there are new challenges that warrant specific attention

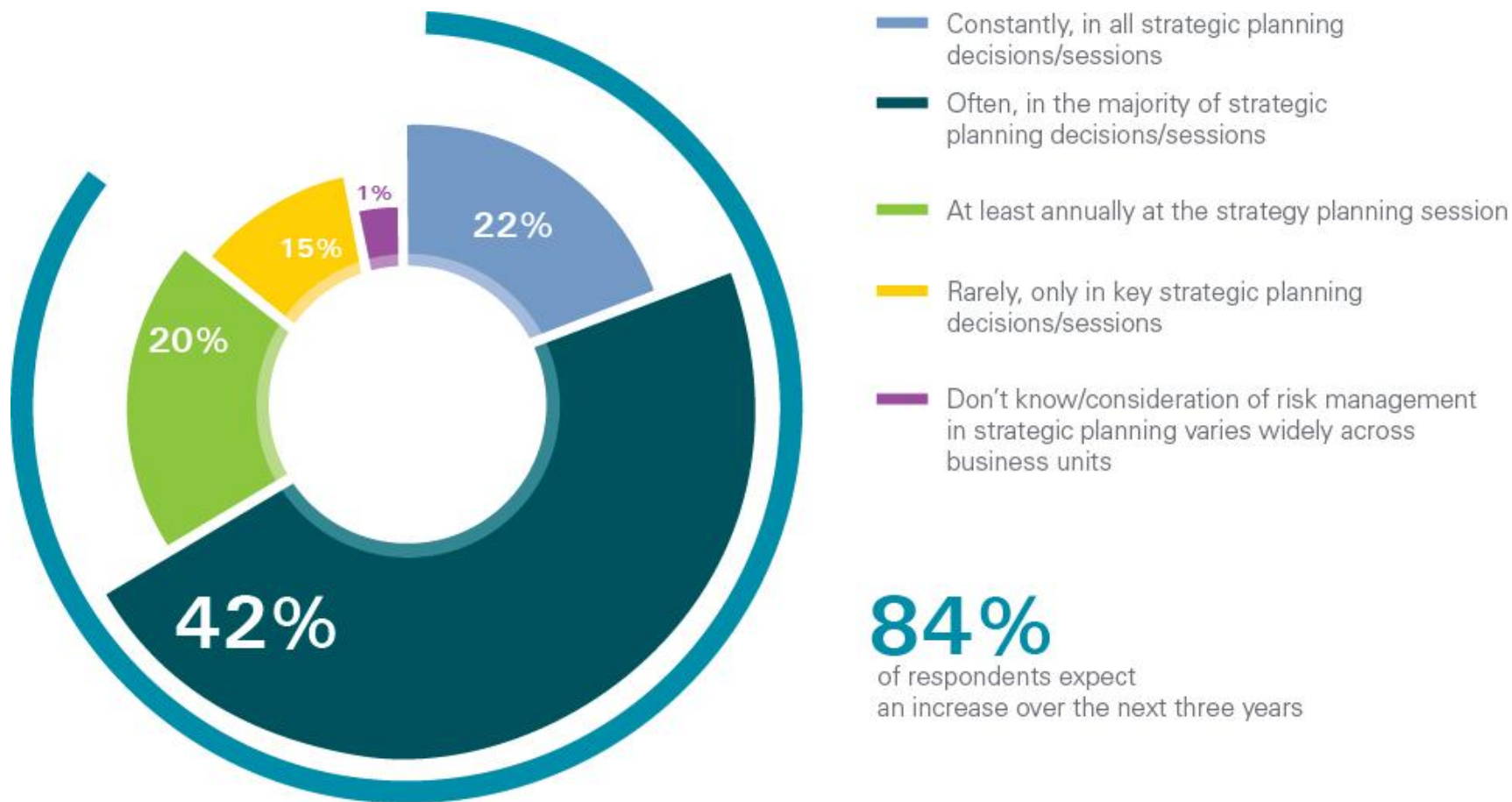
External Drivers Strengthening Risk Management (Past 2 Years)	All–2015	All–2013	All–2011
Increased focus from regulators	38%	34%	38%
Economic volatility	37%	47%	50%
Pressure from customers	26%	20%	18%
Cyber threat environment	22%	N/A	N/A
Pressure from competitors	21%	11%	N/A
Demand from investors for greater disclosure and accountability	20%	22%	22%
Risk events/black swan events	18%	18%	N/A
Large third-party liability losses/litigation	18%	14%	19%
Natural weather events	17%	18%	14%
Political uncertainty	15%	15%	11%
Workforce issues	15%	12%	13%
Pressure from suppliers/vendors	15%	4%	6%
Globalization	11%	N/A	N/A
Other	8%	9%	14%
Random acts of violence	2%	N/A	N/A

# Governance Priorities

- The spotlight on corporate directors will continue to intensify as regulators and investors scrutinize the board's contribution to strategy, risk, and compliance. Bermuda is no exception.
- Drawing on insights from the KPMG global network and our interactions with directors and business leaders over the past 12 months, key considerations that boards should keep in mind include:
  - ❖ Focus on the company's plans to grow and innovate
  - ❖ Reassess the board's role in strategy
  - ❖ Consider whether the board needs to recalibrate how its committees communicate and coordinate on risk oversight
  - ❖ Reassess the company's vulnerability to business interruption, and its crisis readiness
  - ❖ Do we have the right people on the board?
  - ❖ Set the tone and closely monitor leadership's commitment as well as the culture throughout the organization
  - ❖ Promote engagement with shareholders
  - ❖ Sharpen the board's focus on cyber risk and security



# How often are risk management considerations factored into your organization's strategic planning decisions?



Source: Expectations of Risk Management Outpacing Capabilities, KPMG International, 2013.

# The role of the board of directors

- Navigating the myriad of challenges requires an effective approach to enterprise-wide risk management
- The board of directors plays a critical role in overseeing this process.
- The board's focus on effective risk oversight is important to setting the tone and culture towards effective risk management through strategy setting, formulating high level objectives, and approving broad-based resource allocations – “It starts at the Top”
- The COSO Enterprise Risk Management – Integrated Framework highlighted four areas that contribute to board oversight with regards ERM:
  - ❖ Understanding the entity's risk philosophy and concur with the entity's risk appetite
  - ❖ Know the extent to which management has established effective enterprise risk management of the organization
  - ❖ Review the entity's portfolio of risk and consider it against the entity's risk appetite
  - ❖ Be apprised of the most significant risks and whether management is responding appropriately

# The Upside of Risk Oversight

- The “new normal” of low growth will likely continue to challenge companies in 2015
- The growth conundrum is a particular challenge for this generation of business leaders who, having gone through the financial crisis, are inclined to be more risk averse
- In this environment, boards have a critical role to play in helping the company not only avoid missteps, but also take smart risks to grow, innovate, and stay competitive
- However, this will require some new skills
  - ❖ The complex, volatile, and uncertain business environment today has made the “annual review and concur” model of the board’s oversight of strategy obsolete.
  - ❖ Globalization, new technologies, upstart competitors, and all the “what-ifs” looming around the bend require a frank reassessment of the board’s role in strategy
- One of those new skills will be around cyber

# Cyber Risk Oversight

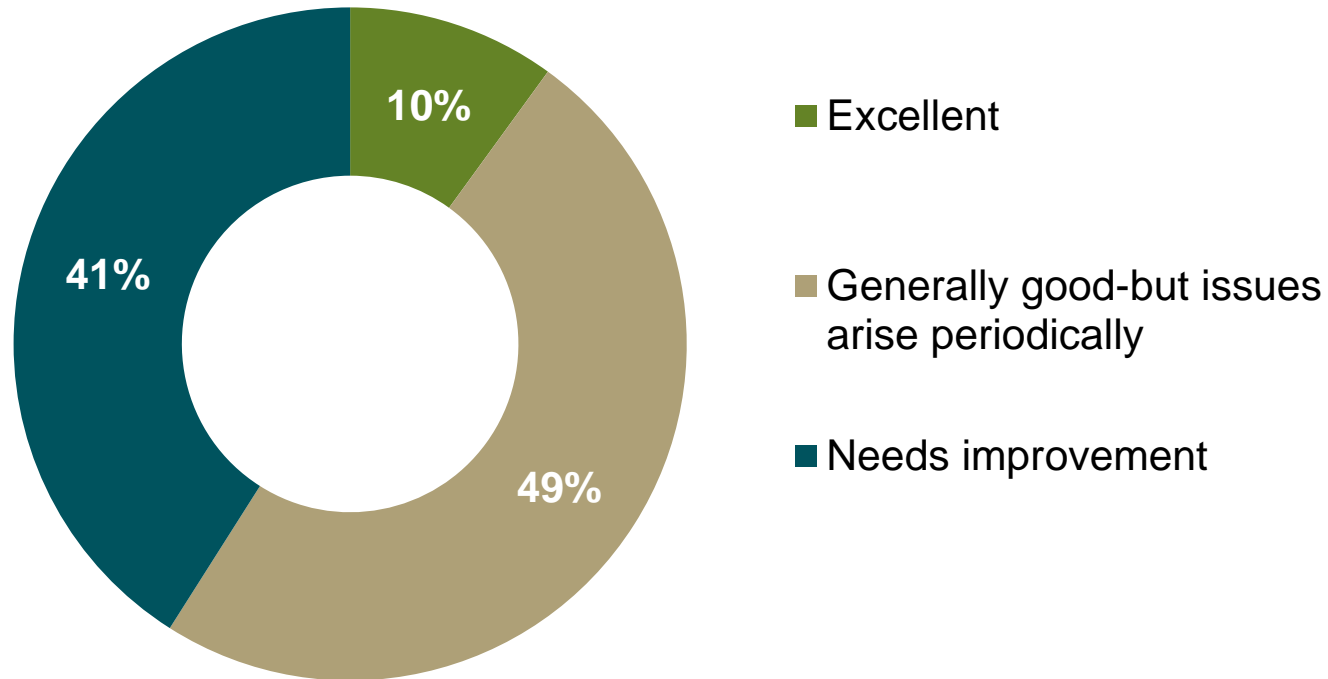
- Increasing threats to corporate information systems and intellectual property – as well as compliance risks, the potential for lawsuits, reputational damage, and loss of customers – have elevated cybersecurity to the board level and as a critical business priority (where it should be).
- Regulators worldwide have sharpened their scrutiny of companies' data security efforts, as well as disclosures and communications about cybersecurity risks and breaches
- Ensuring the adequacy of a company's cyber defenses needs to be a critical aspect of risk management and oversight.
- Is cybersecurity risk given regular and adequate time on the board's agenda?
- What are our biggest vulnerabilities and our most critical data sets?
- What are the results of our most recent penetration tests and external assessments of our cyber defences?
- Do we have a cyber-incident response plan?

# Cyber Security







# Quality of Information

Please rate the quality of the information you receive about cyber security—including data privacy and the protection of intellectual property:



Source: "KPMG 2014 Audit Committee Member Survey".

# Cyber Security Findings in Global ACI Survey

-  Rated as 9th highest as posing greatest challenge to the company
-  Rated as 3rd highest area that the audit committee should devote time to in 2015 versus 2014
-  Rated last for quality of information received of top 12 risks
-  Rated second last for quality of interaction of function with audit committee

# We are in the midst of a digital and mobile revolution



More than 90 percent of the world's data has been created in the past two years

- **DIGITAL and MOBILE technologies are transforming the way we live and work.**



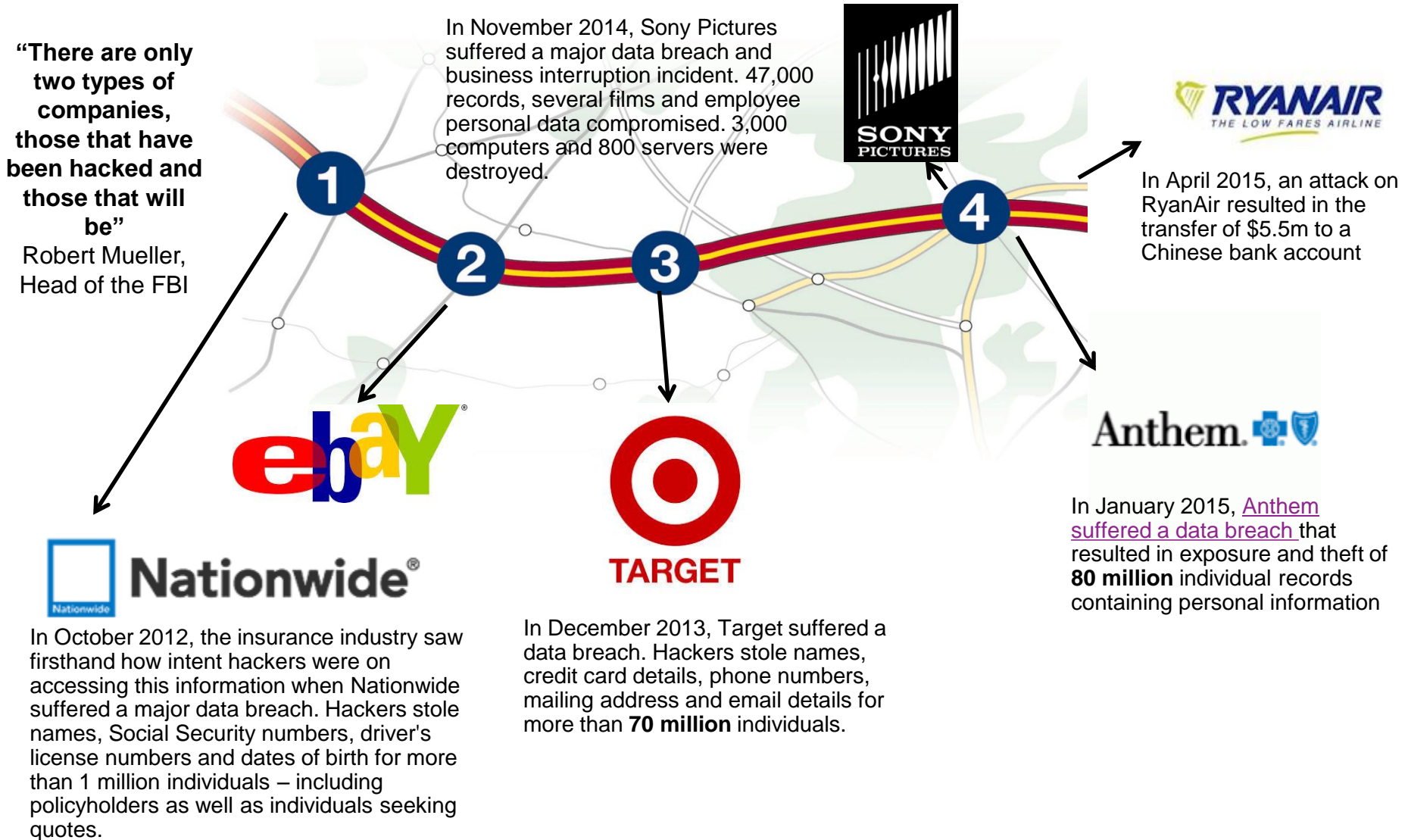
**of companies are in some phase of CHANGING THEIR BUSINESS MODEL\***

\* 2013 KPMG Technology Innovation & Business Transformation Surveys

# Cyber Security Concerns Are The “New Normal”

“There are only two types of companies, those that have been hacked and those that will be”

Robert Mueller, Head of the FBI



# The Sony Cyber Attack – Cyber Context

If you want to talk about state-of-the-art hacking or what's going on in the international cyber arms market, Jon Miller's [a good place to start](#). He turned down a job with the NSA and a government car while he was still in high school, because he says he was already making more money doing private consulting work and honing his skills as a penetration tester.

- Steve Kroft: So you're a hacker?
- Jon Miller: I was. Now I'm, you know, a computer security professional. But yeah, I mean, for the majority of my career I was an ethical hacker, where I would actually go out and hack companies and then work with them to make sure they didn't get hacked by somebody else.
- Since Miller says he's been well-paid to hack into nuclear power plants by utility companies, we wanted to know what he thought about the Sony attack and the malware the North Koreans used to pull it off.
- Steve Kroft: If I set you down and gave you a pencil and paper and said, "Write a list of a dozen people that could do this."
- Jon Miller: Oh yeah, I mean, there are way more than a dozen people. There are probably three, four, five thousand people that could do that attack today.

Source: "CBS, 60 Minutes North Korean Cyber Attack on Sony".

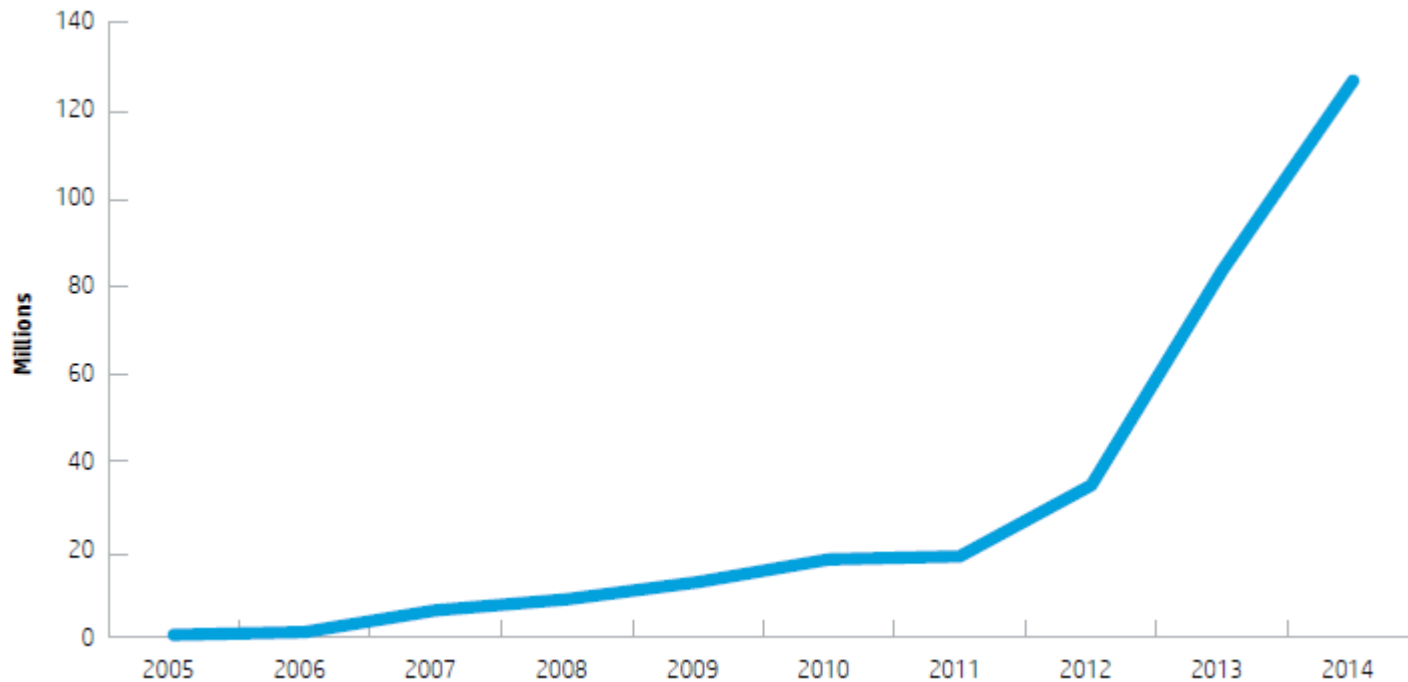
# Quantifying the Cyber threat

- The Global State of Information Security Survey 2015 found that the number of recorded security incidents has “increased 66% year-over-year since 2009”, to a total of 42.8 million in 2014 – a figure that doesn’t cover the vast number of unreported or undetected incidents
- UK Government Dept. of Business Innovation and Skills report that 60% of UK SMEs had a security breach in 2014
- Lloyd’s of London CEO Inga Beale estimates that cyber attacks have cost businesses up to \$400 billion a year
- The Center for Strategic and International Studies estimates that the annual cost of cyber crime is as high as \$445 billion
- The Aon 2015 Global Risk Management Survey includes Cyber for the first time at number 9 and predict it to rise to number 7 in 2016



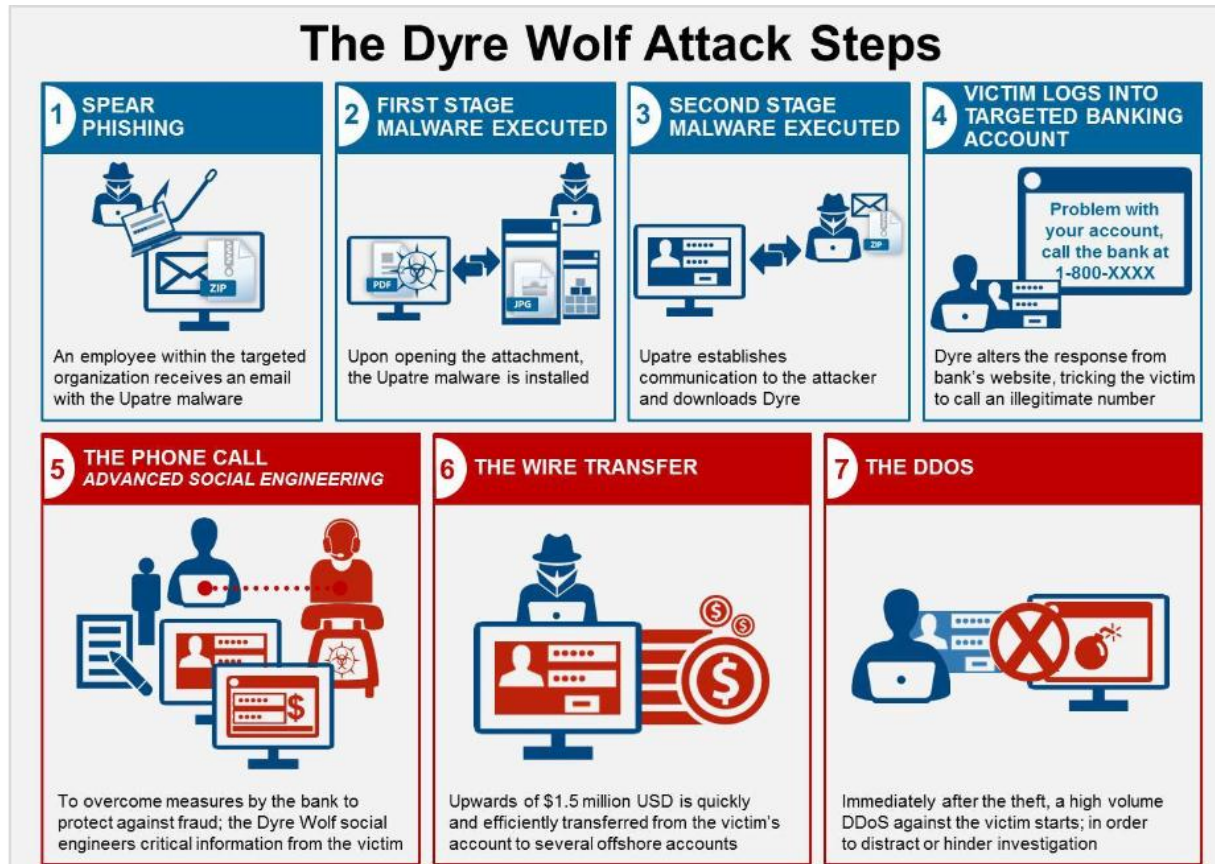
# The Cyber threat is rapidly expanding

**Problem:** 140 million unique Windows malware samples collected in 2014



# Anatomy of a Cyber Attack

## Threat Intelligence: 'Dyre Wolf' 2015



# Key (Security) Trends

1

## External Threats

Organized crime, nation-states, cyber espionage, hacktivism, insider threats.

2

## Change in the way business is conducted

Cloud computing, big data, social media, consumerization, BYOD, mobile banking.

3

## Rapid technology change

Critical national infrastructure, smart/metering, internet of all things.

4

## Regulatory compliance

Data loss, privacy, records management.

5

## Changing market and client need

Strategic shift, situational awareness, intelligence sharing, cyber response.

# New “Vectors” of Threats are Accelerating the Concern

## YESTERDAY...

### Bad “Actors”

- ▶ Isolated criminals
- ▶ “Script Kiddies”

“Target of Opportunity”

### Targets

- ▶ Identity Theft
- ▶ Self Promotion Opportunities
- ▶ Theft of Services

## TODAY...

### Bad “Actors”

- ▶ Organized criminals
- ▶ Foreign States
- ▶ Hacktivists

“Target of Choice”

### Targets

- ▶ Intellectual Property
- ▶ Financial Information
- ▶ Strategic Access

# Cyber Regulation

- European Union Cyber Security Strategy (December 2013)
  - General Data Protection Regulation (GDPR) set to be finalized in early 2015, with compliance becoming mandatory in 2017. Max penalty for serious breach of €100m, or 5% of annual global turnover
  - Network and Information Security (NIS) directive is due for implementation in 2015 and will impose new security and incident reporting requirements on a broader range of private sector companies.
- U.S. Securities and Exchange Commission, Division of Corporate Finance – October 2011, disclosure guidance for situations related to cybersecurity risks and incidents
- U.S, National Cybersecurity and Critical Infrastructure Protection Act, 2013.
- NIST, Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework). February 2014. In response to the Executive Order from President Barack Obama that tasked it with addressing how to protect critical infrastructure sectors the previous February
- Several Industry Specific Initiatives:
  - Commodity Futures Trading Commission, DSIO Best Practices for securing financial information (Feb. 26, 2014) under Title V of the Gramm-Leach-Bliley Act
  - New York State Department of Financial Services - Extended IT/cyber security examinations and risk assessments under Insurance Law Sections 308 and 1504(a). (March 2015)
  - Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Risk Alert: OCIE Cybersecurity Initiative (April 15, 2014) (“April 2014 Risk Alert”)
  - Financial Industry Regulatory Authority, Report on Cybersecurity Practices (February 2015)
  - Securities and Exchange Commission, Division of Investment Management, IM Guidance Update (April 2015), No. 2015-02, “Cybersecurity Guidance” (“Guidance Update”).

# Lack of threat intelligence impact on organizations

**\$10M is the average amount spent** in the past 12 months to resolve the impact of exploits...

Actionable intelligence about cyber attacks within 60 sec of a compromise could **reduce cost by 40%...**

**57% say the intelligence currently available** to their enterprises is often **too stale** to enable them to grasp

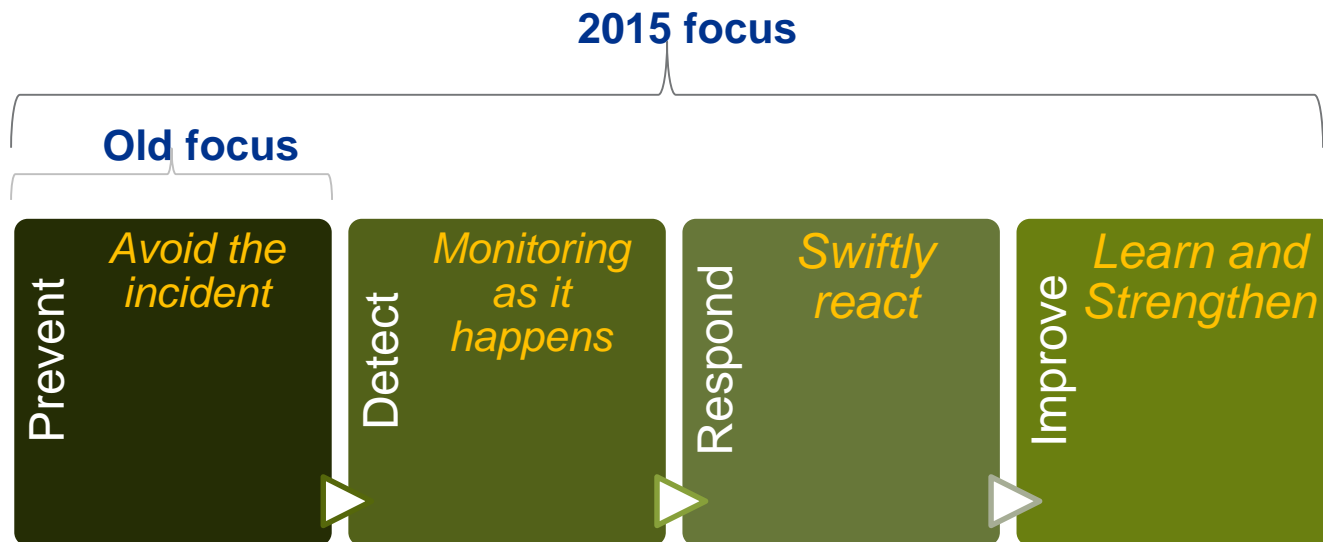
**Only 10% know with absolute certainty** that a material exploit or breach to networks or enterprise systems occurred

**23% said it can take as long as a day** to identify a compromise

**49% said it can take within a week to more than a month** to identify a compromise

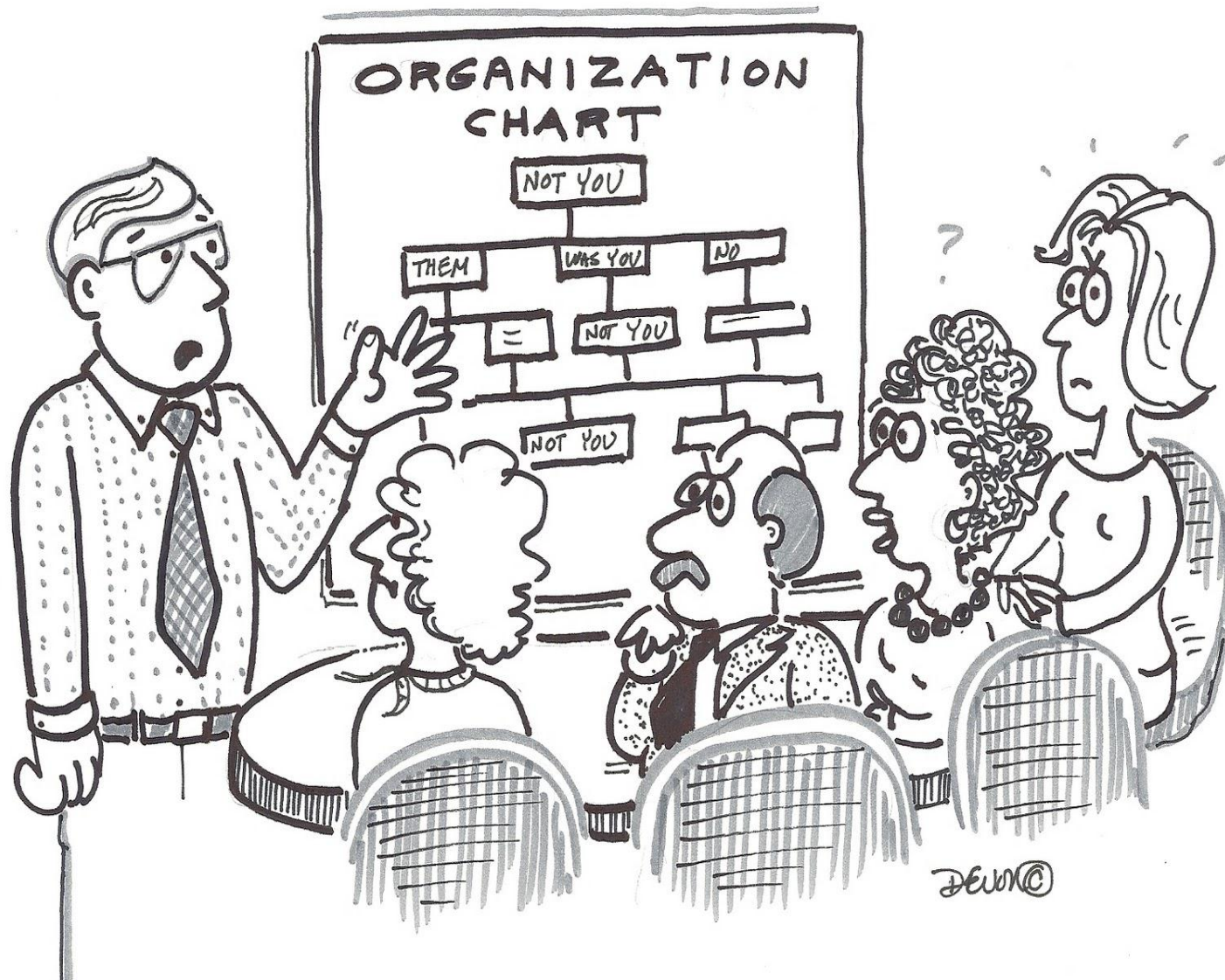


# Focus Shift



# Key Stakeholder Analysis

# Who is responsible for cyber security?



# Key Stakeholder Analysis

## Board/CEO

The Board/CEO should ask: “Are we organized appropriately?”

Key Task of Board/CEO	Details and Commentary
<p><b>Review and refine information governance structure</b></p>	<ul style="list-style-type: none"> <li>■ Assign distinct board committee responsibility for information privacy and security</li> <li>■ Establish management responsibilities; require ongoing reporting, monitoring and review of information risks and controls</li> <li>■ Provide adequate budget and operational resources</li> <li>■ Consider appointing CISO (chief information security officer) and CPO (chief privacy officer)</li> <li>■ Develop and approve appropriate cyber security protocols and safeguards; increase internal awareness</li> <li>■ <b>Evaluate cyber-insurance coverage</b></li> <li>■ <b>Evaluate deployment of best practices and available tools, safeguards and patches</b></li> </ul>
<p><b>Develop cyber security and data protection risk assessment and implement preventative measures</b></p>	<ul style="list-style-type: none"> <li>■ Understand system and network vulnerabilities; plan for possible “persistent” threats</li> <li>■ <b>Understand exposure to third parties and service providers (includes cloud providers and law firms)</b></li> <li>■ Keep highly sensitive data offline</li> <li>■ Put a firewall curtain around vulnerable locations (e.g., China)</li> <li>■ Proactively hunt for intruders within own networks</li> </ul>
<p><b>Monitoring environment</b></p>	<ul style="list-style-type: none"> <li>■ Monitor legislative, policy, industry, contractual, litigation, marketplace, consumer and employee developments and expectations</li> <li>■ Address legal compliance and reporting responsibilities</li> <li>■ Consider SEC issues</li> </ul>

# Key Stakeholder Analysis

## Board/CEO (cont'd)

**Boards often say they lack proper security metrics and have difficulty measuring the value of security**

Key Task of Board/CEO	Details and Commentary
<p><b>Ensure adequate support and resources (e.g., committees) and allocate responsibilities accordingly</b></p>	<ul style="list-style-type: none"> <li>■ Full Board is responsible for risk management oversight in general</li> <li>■ Responsibility for cyber security typically delegated to a Board committee (e.g., Audit, Risk or Technology)</li> <li>■ Consider committee workloads and expertise of directors (e.g., IT experience)</li> <li>■ Deep dive annually and quarterly status reports</li> <li>■ Require management to provide specific reports on cyber risks, incidents, activities and business impact quantification; similar to compliance reporting</li> <li>■ Committee reviews with full Board annually</li> <li>■ Reserve adequate time on Board meeting agendas for cyber security               <ul style="list-style-type: none"> <li>– Receive quarterly reports on cyber risks, incidents and activities</li> <li>– Discuss as part of strategy discussions if IT is critical</li> </ul> </li> <li>■ <b>Consider delegating primary oversight of cyber security to a committee</b></li> <li>■ Conduct in-depth audit of IT policies and cyber security programs, including incident response plan, at least annually</li> <li>■ Review budgets and increase IT resources/spending if necessary</li> <li>■ <b>Engage third-party cyber security experts as needed</b></li> <li>■ <b>Educate a tech-savvy director on cyber security or consider recruiting a new director with IT or cyber risk expertise</b></li> <li>■ <b>Evaluate adequacy of cyber liability insurance coverage</b></li> </ul>
<p><b>Assign responsibility for managing and monitoring cyber risk to a C-level executive</b></p>	<ul style="list-style-type: none"> <li>■ Consider appointing a Chief Information Security Officer (CISO) and a Chief Privacy Officer in addition to the Chief Information Officer</li> <li>■ Person who develops cyber security policies and programs (often the CIO) should not also audit them</li> <li>■ CISO may have a direct reporting line to the Board/Committee</li> <li>■ CISO should manage the cyber incident tracking protocol that is reviewed by the Board/Committee</li> </ul>

# Key Stakeholder Analysis

## CIO/CISO

Security function and CISO role need to quickly evolve, focusing more on business and less on technology

### Key Considerations for CIO/CISO

- **Must ensure that the company has a comprehensive and customized incident response team and plan**
- **Cross-functional incident response team**
  - IT, Compliance, Corporate Communications, Legal, Finance
- **Incident response plan**
  - Anticipate common cyber attack scenarios and develop preventative and responsive measures for each
  - Require action within hours, not days, to reduce impact
- **Develop reporting mechanisms**
  - Clarify which incidents require immediate Board notification
  - Require periodic testing of the plan



# Key Stakeholder Analysis

## CIO/CISO (cont'd)

With the evolving cyber threat landscape, many CISOs face a variety of challenges; CISOs cite gaps in skill sets on their teams, lack of bandwidth and inadequate budgets as some of the biggest issues

### Emerging Risks

- Targeted Malware Attacks/Spearphishing
- Intellectual Property Protection
- BYOD/Consumerization
- Foreign National Threats
- Increased Data Leakage and Portability
- “Zero Day” Attacks
- Insider Threats
- Diverse Compliance Challenges
- Critical Infrastructure Protection
- Integration with ERM Initiatives

### Technical Architecture

- Security Analytics & Threat Intelligence
- Public/Private “Cloud” Computing
- Incident Response & Logging
- GRC Solutions and Integration
- Application and Code Review
- Data Loss Prevention
- IAM Governance and Process (Role Optimization, Privileged Management)
- Increased Encryption (Data Level and Mobile)
- Endpoint Protection & Validation

### Business Enablement

- Rapidly Changing Business Needs
- Increased Value Chain Integration
- Globalization
- Expanding New Revenue Streams
- Mergers, Sourcing and Workforce Changes
- Need for Improved Business Intelligence
- E-Discovery and Investigations
- Social Media Platforms

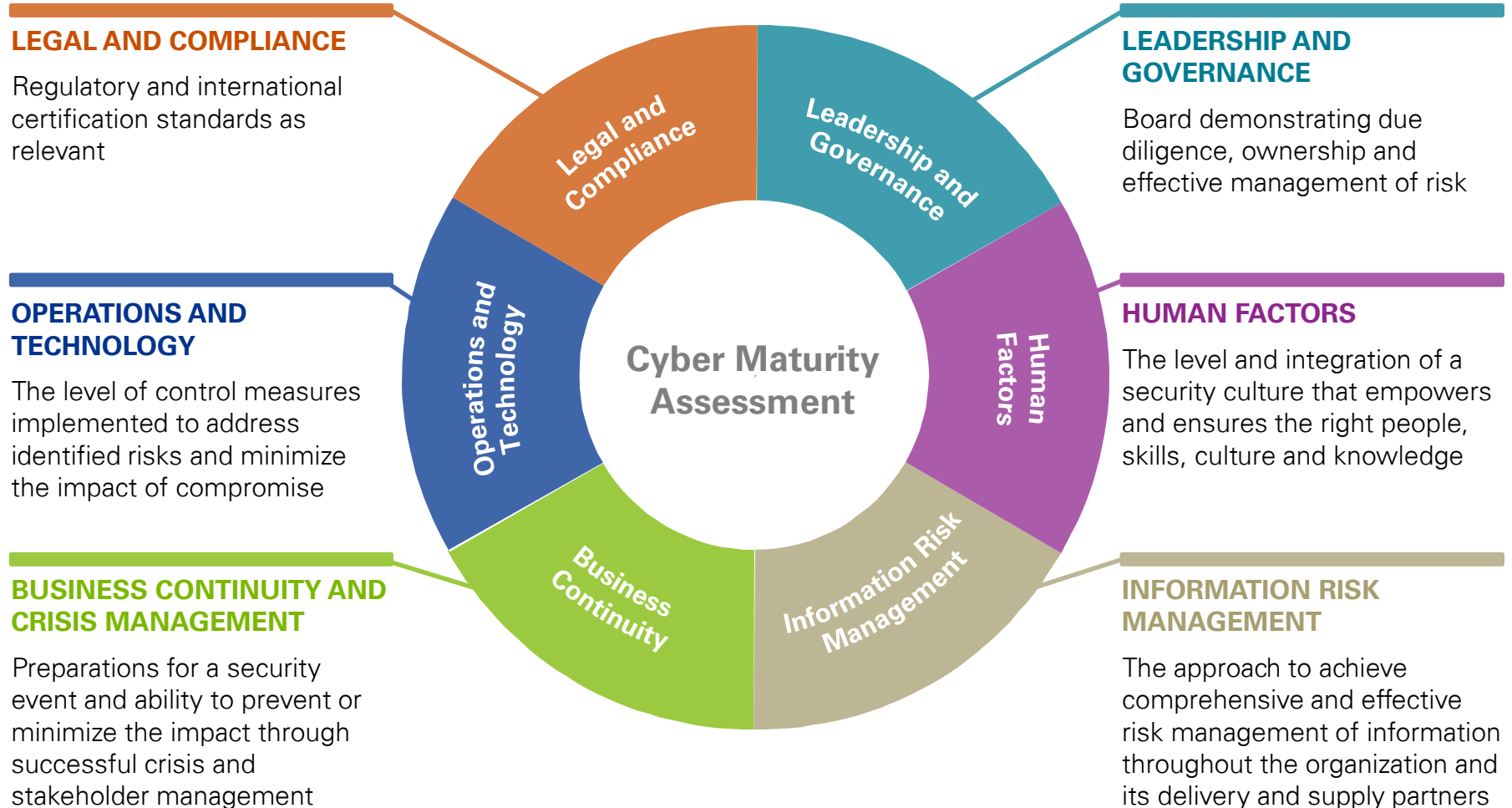
### Security Management

- Better Integration with Risk Management
- Security Organization Model and Structure
- Awareness and Training
- Crisis Management
- “Doing More with Less”
- Vendor and 3rd Party Management
- Asset and Configuration Management
- Executive Reporting and Metrics
- Managed Security Services

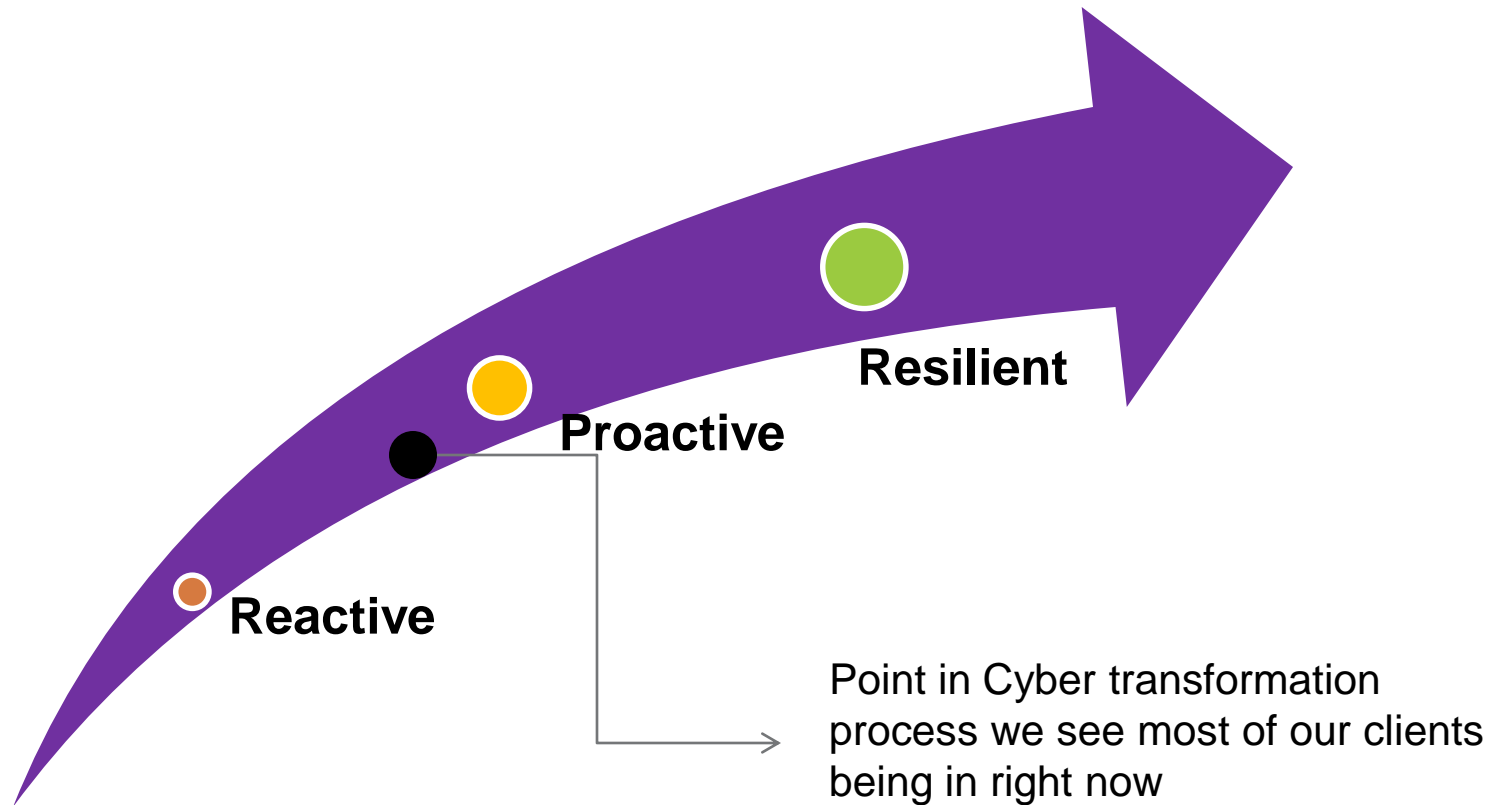


# Assessing Cyber Maturity/Readiness

# Cyber Readiness: Six Key Maturity Areas To Focus On



# “From Data Center To Boardroom” - How Do Risk Management Considerations Relate To Cyber Security?



1 = “Initial” / “Reactive”

2 = “Established” / “Proactive”

3 = “Business Enabling” / “Resilient”

# Is leadership enabling appropriate measures?

## Leadership and governance

Board demonstrating due diligence, ownership, and effective management of risk

## Human factors

The level and integration of a security culture that empowers and ensures the right people, skills, culture, and knowledge

## Topics

Understanding of Cyber

Board Involvement

Third-Party Supplier Relationships

Identification of Critical Data

Ownership and Governance for Data Protection

Program Management

## Topics

Training and Awareness

Culture

Personnel Security Measures

Talent Management

Organizational Roles and Responsibilities

# Questions







*cutting through complexity*

# Regulatory Update



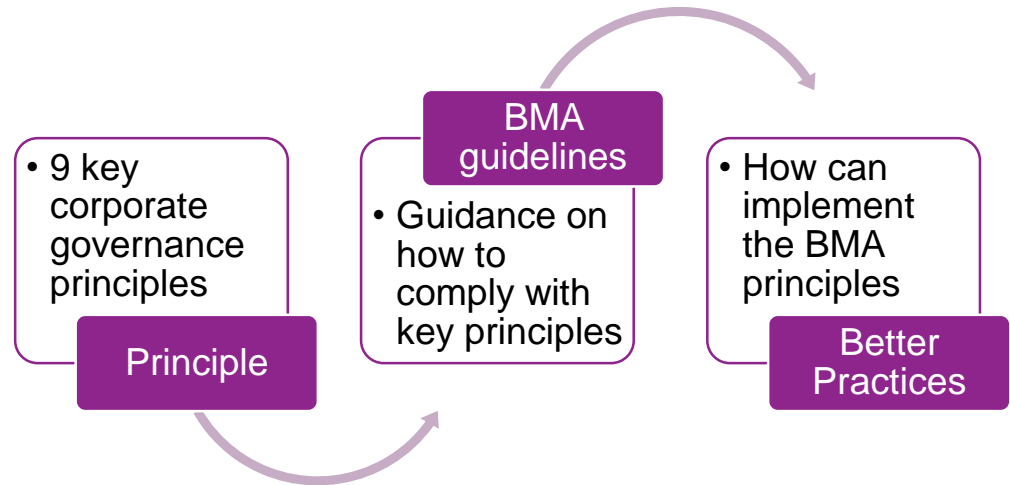


# The World We Live in....





# Bermuda Corporate Governance Regulatory Developments



- Insurance – Code of Conduct (revised) – December 2014
- Banking – Statement of Principals – December 2012
- Trust, Investment Businesses and Fund Administrators – January 2014

# Corporate Service Provider Regulatory Changes



- Corporate Service Provider Business Act 2012
- Corporate Service Provider Business Amendment Act 2012
- Transition period expected to end April 1, 2016

# FATCA Update – Things that should be in the rear view mirror

Entity Classification



Early 2014

FATCA Registration


30 June 2014 – Model 2 IGA or no IGA  
31 December 2014 – Model 1 IGA

Policies and procedures

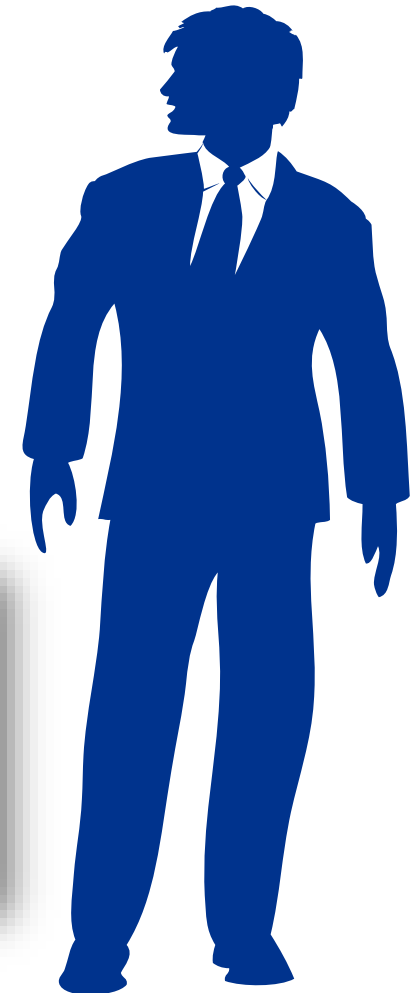


30 June 2014

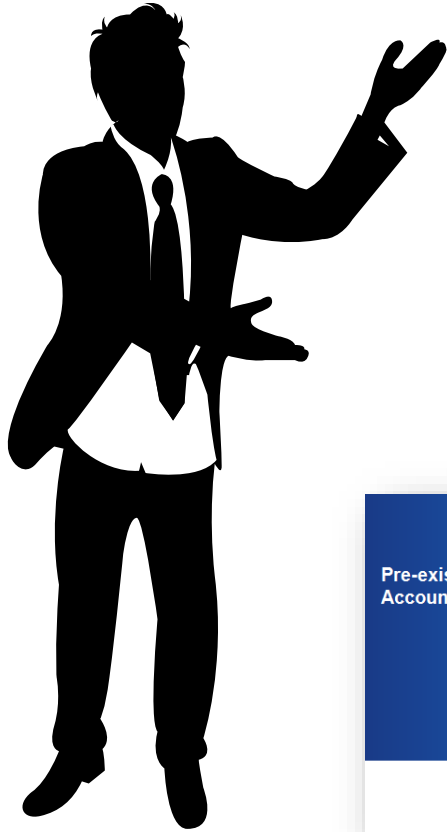
New Accounts (Onboarding)



1 July 2014  
or  
1 January 2015



# FATCA Update – Things still to be done



Pre-existing Accounts

An icon showing a computer monitor with a pie chart and a smartphone with binary code (01010110) on its screen.

30 June 2015  
30 June 2016

Reporting

An icon showing three stylized human figures sitting around a table, representing a meeting or reporting session.

31 December 2014  
reporting due:

- Bermuda June 2015
- BVI June 2015
- Cayman May 2015

Common Reporting Standard

The logo for the OECD (Organisation for Economic Co-operation and Development), featuring a globe and the acronym "OECD".

1 January 2016

FATCA Compliance Program

An icon showing two hands shaking, symbolizing an agreement or a compliance program.

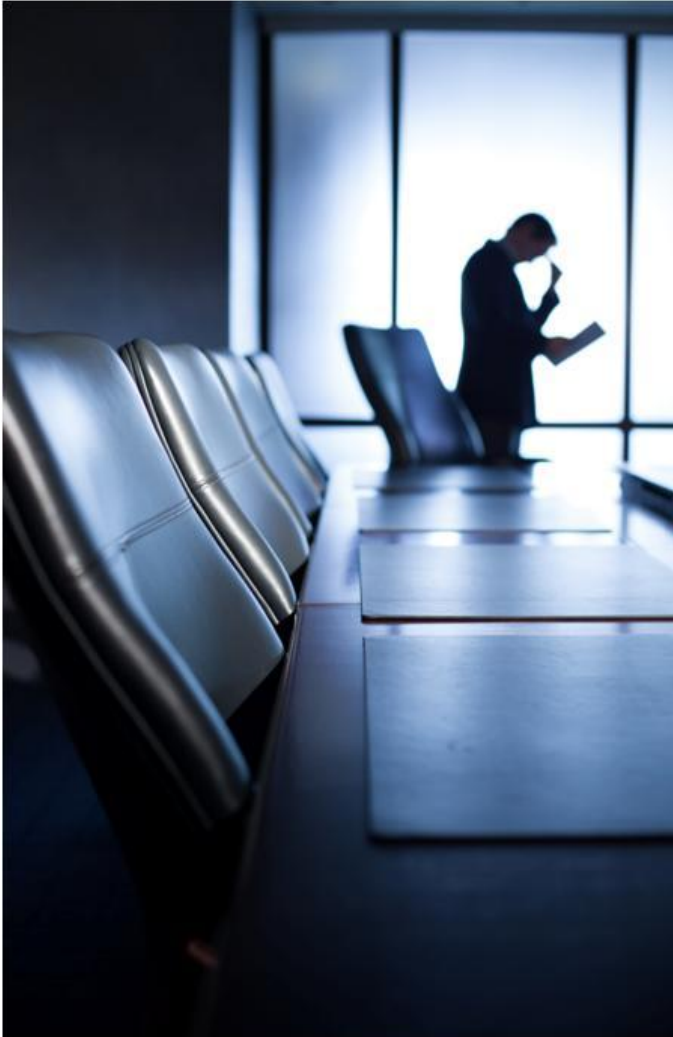


# Anti Money Laundering (AML) Update



- Changes are proposed to bring Bermuda’s AML/ATF legislative framework into full compliance with the Financial Action Task Force (FATF) 2012 Revised 40 Recommendations.
  
- A few of the key changes you should be aware of are detailed below. The Bermuda regulations are to be amended to;
  - Clearly state EDD will be required for countries identified by FATF as high risk as well as a duty to do EDD when a country is otherwise considered a high risk;
  - Expand of the definition of PEPs to include domestic PEPs and officers of international organizations;
  - Expressly provide that with respect to third party reliance relationships the information must be “immediately” available;
  - Require a documented business risk assessment, that is keep it up-to-date and available to share with competent authorities;
  - Not only make it a requirement to obtain information on the purpose and intended nature of the business relationship; but to take reasonable steps to understand the business relationship; and
  - Require independent testing of your AML compliance framework and the effectiveness of your AML compliance program.

# EU AIFM Directive



- The Alternative Investment Fund Managers Directive ('AIFMD') is an extra-territorial EU Directive that regulates the marketing of Alternative Investment Funds ("AIFs") to EU investors.
- The Directive came in to effect on 22 July 2013, with a transitional year being granted for managers to reach compliance.
- Non compliance with the Directive could result in regulatory sanction and investor recourse.
- The marketing passport
- Private placement
- Reverse solicitation

# Insurance – BMA activities in 2015



- Final EIOPA equivalence assessment
- Economic Balance Sheet
  - Data
  - Processes and controls
  - Validation
- Enhancements to the regime for commercial insurers and groups
- Enhanced reporting for captives

# Banking – BMA activities in 2015



- Implementation of Basel III
  - Quantity and quality of capital (phased in)
  - Leverage ratio
  - Liquidity coverage ratio (phased in)
- Introduction of Special Resolution Regime
- Deposit Insurance Scheme



# Any questions?





*cutting through complexity™*

# Thank you

© 2015 KPMG, a group of Bermuda limited liability companies which are member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.