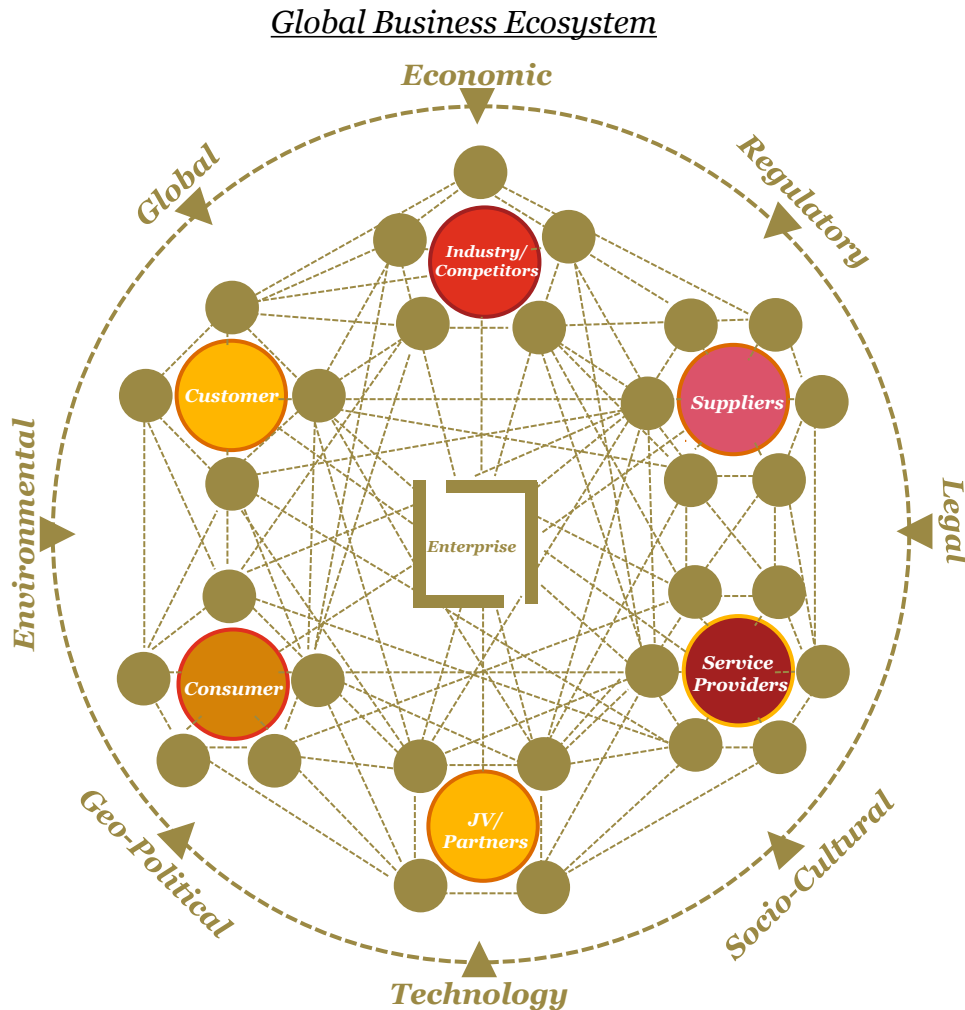


PwC Cybersecurity Briefing

June 25, 2014

The views expressed in these slides are solely the views of the presenters and do not necessarily reflect the views of the PCAOB, the members of the Board, or the Board's staff. The PCAOB makes no representation as to the accuracy or completeness of this information.

The cyber challenge now extends beyond the enterprise



The Evolution:

- Technology-led innovation has enabled business models to evolve
- The extended enterprise has moved beyond supply chain and consumer integration
- Connectivity and collaboration now extends to all facets of business

Leading to:

- A dynamic environment that is increasingly interconnected, integrated, and interdependent
- Where changing business drivers create opportunity and risk

Scope of cybersecurity – Technology types



**Information
Technology**

Computing resources and connectivity for processing and managing data to support organizational functions and transactions



**Operational
Technology**

Systems and related automation assets for the purpose of monitoring and controlling physical processes and events or supporting the creation and delivery of products and services



**Consumer
(Products and Services)
Technology**

Computing resources and connectivity integrated with or supporting external end-user focused products and services

● **Cybersecurity** encompasses all three **technology types**

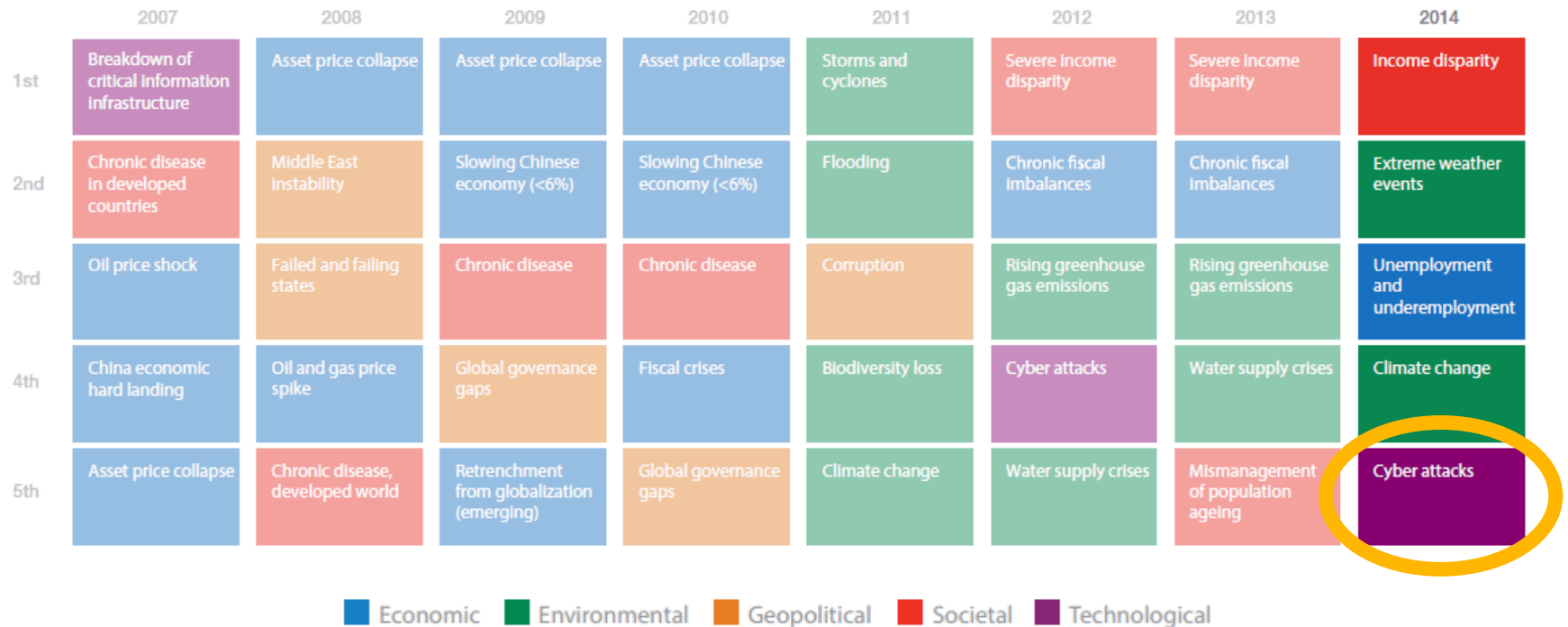
Evolving perspectives

Considerations for businesses adapting to the new reality

	Historical IT Security Perspectives	➔	Today's Leading Cybersecurity Insights
Scope of the challenge	<ul style="list-style-type: none">• Limited to your “four walls” and the extended enterprise		<ul style="list-style-type: none">• Spans your interconnected global business ecosystem
Ownership and accountability	<ul style="list-style-type: none">• IT led and operated		<ul style="list-style-type: none">• Business-aligned and owned; CEO and board accountable
Adversaries' characteristics	<ul style="list-style-type: none">• One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain		<ul style="list-style-type: none">• Organized, funded and targeted; motivated by economic, monetary and political gain
Information asset protection	<ul style="list-style-type: none">• One-size-fits-all approach		<ul style="list-style-type: none">• Prioritize and protect your “crown jewels”
Defense posture	<ul style="list-style-type: none">• Protect the perimeter; respond <i>if</i> attacked		<ul style="list-style-type: none">• Plan, monitor, and rapidly respond <i>when</i> attacked
Security intelligence and information sharing	<ul style="list-style-type: none">• Keep to yourself		<ul style="list-style-type: none">• Public/private partnerships; collaboration with industry working groups

The World Economic Forum ranked cyber attacks as one of the top 5 most likely risks in 2014

Top 5 Global Risks in Terms of Likelihood



Source: World Economic Forum Global Risks 2014

Summary findings from US State of Cybercrime Survey

1. Spending with a misaligned strategy isn't smart

Strategy should be linked to business objectives, with allocation of resources tied to risks.

- **38%** prioritize security investments based on risk and impact to business

2. Business partners fly under the security radar

Recent contractor data leaks and payment card heists have proved that adversaries can and will infiltrate systems via third parties, but most organizations do not address third-party security.

- **44%** have a process for evaluating third parties before launch of business operations
- **31%** include security provisions in contracts with external vendors and suppliers

3. A missing link in the supply chain

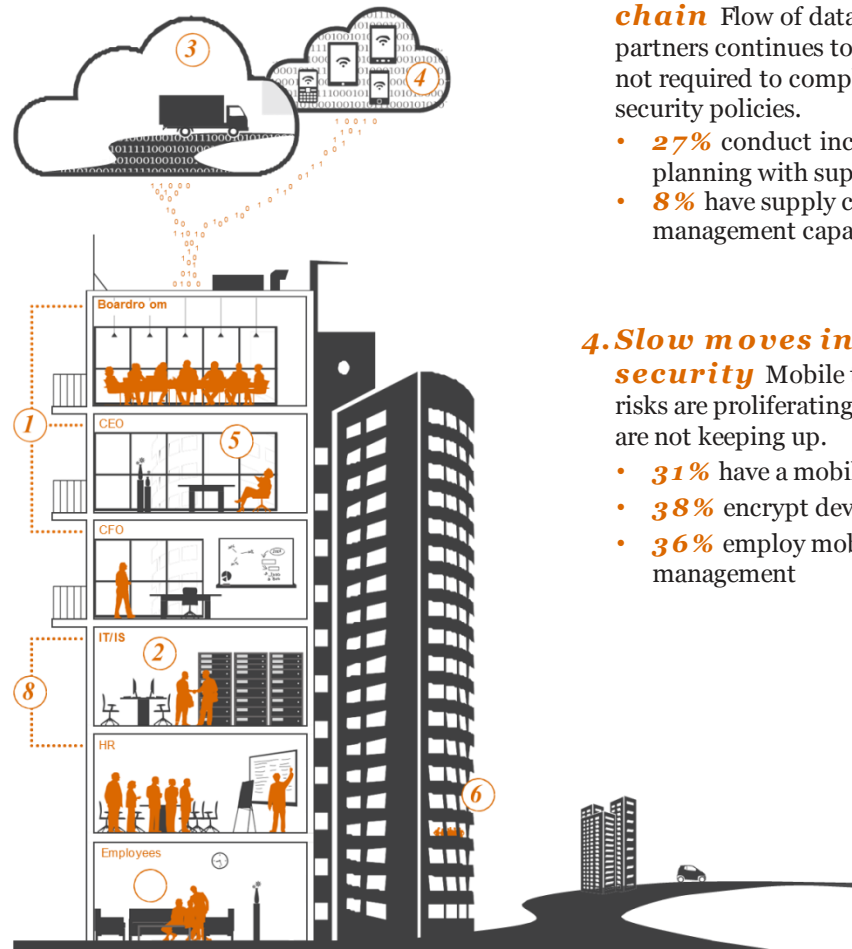
Flow of data to supply chain partners continues to surge, yet they are not required to comply with privacy and security policies.

- **27%** conduct incident-response planning with supply chain partners
- **8%** have supply chain risk-management capability

4. Slow moves in mobile security

Mobile technologies and risks are proliferating but security efforts are not keeping up.

- **31%** have a mobile security strategy
- **38%** encrypt devices
- **36%** employ mobile device management



1. PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2014, September 2013

Summary findings from US State of Cybercrime Survey (cont.)

8. Untrained employees drain revenue

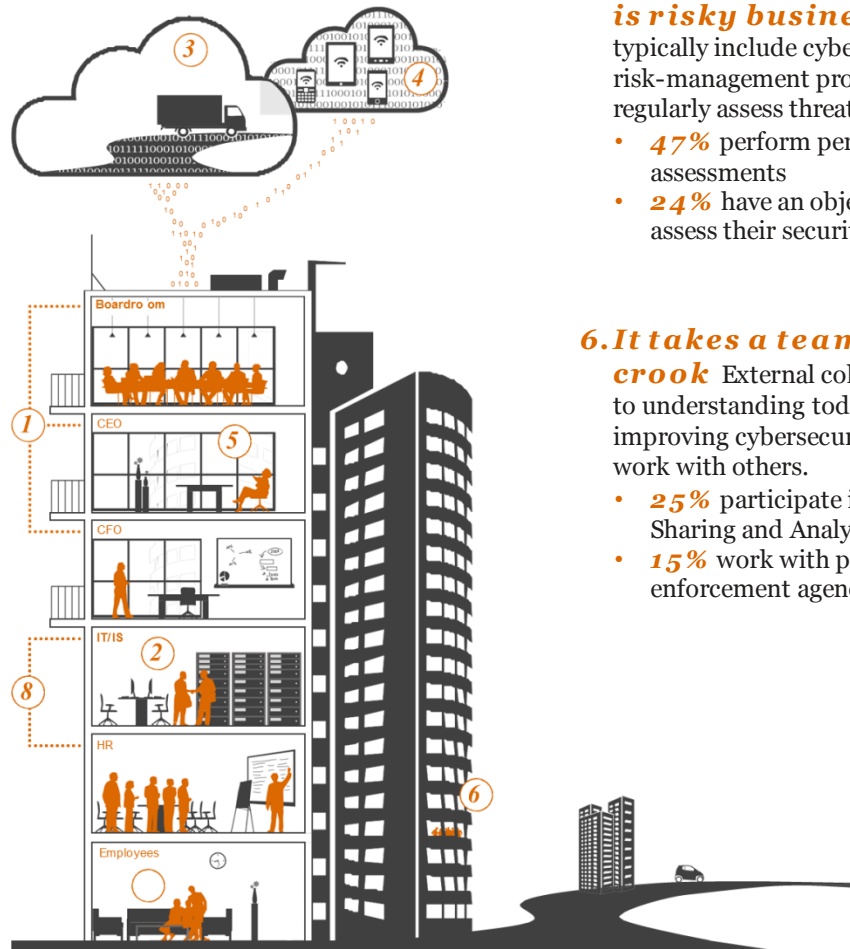
Employee vulnerabilities are well known, but businesses do not train workers in good cybersecurity hygiene.

- **20%** train on-site first responders to handle potential evidence
- **76%** less is spent on security events when employees are trained, yet
- **54%** do not provide security training for new hires

7. Got suspicious employee behavior?

Cybersecurity incidents carried out by employees have serious impact, yet are not addressed with the same rigor as external threats like hackers.

- **49%** have a formal plan for responding to insider events
- **75%** handle insider incidents internally without involving legal action or law enforcement



5. Failing to assess for threats is risky business

Organizations typically include cyber risks in enterprise risk-management programs but do not regularly assess threats.

- **47%** perform periodic risk assessments
- **24%** have an objective third party assess their security program

6. It takes a team to beat a crook

External collaboration is critical to understanding today's threats and improving cybersecurity but most don't work with others.

- **25%** participate in Information Sharing and Analysis Centers (ISACs)
- **15%** work with public law enforcement agencies

1. PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2014, September 2013

Evolving business risks...

...impacting brand, competitive advantage, and shareholder value

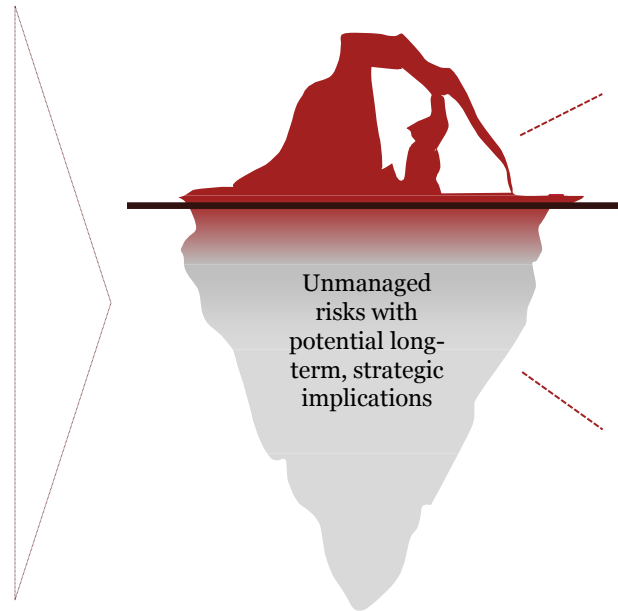
Highlights of activities impacting risk:

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*



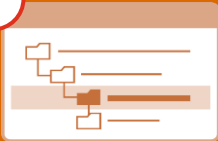




Historical headlines have primarily been driven by compliance and disclosure requirements

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

Steps organizations can take to address cybersecurity risks

Organizations can't eliminate the risk of cyber attack, but they can minimize its consequences. Here are 5 things leading organizations do to combat cybersecurity risks.

- **1**
Own
 - Cyber risk is owned by leadership and is not relegated to the IT department.
 - Periodic cybersecurity briefings are provided to the Board and C-Suite.
- **2**
Prioritize
 - Leadership prioritizes and monitors cybersecurity investments.
 - Investments are made in new capability, not just technology.
 - Crown jewels have been identified and their protection prioritized.
- **3**
Learn and Incorporate
 - Leading organizations work with various external parties, share information on current threats and incorporate learnings into their own cybersecurity monitoring initiatives.
- **4**
Culture and Awareness
 - A security culture and mindset is reinforced through testing and training so all employees, including the C-Suite, understand their role in protecting information assets.
- **5**
Secure
 - All technology domains and high-risk interconnection points are continually assessed and secured, control systems, product development, 3rd parties, the supply chain, mobile devices and the cloud.

Thank You