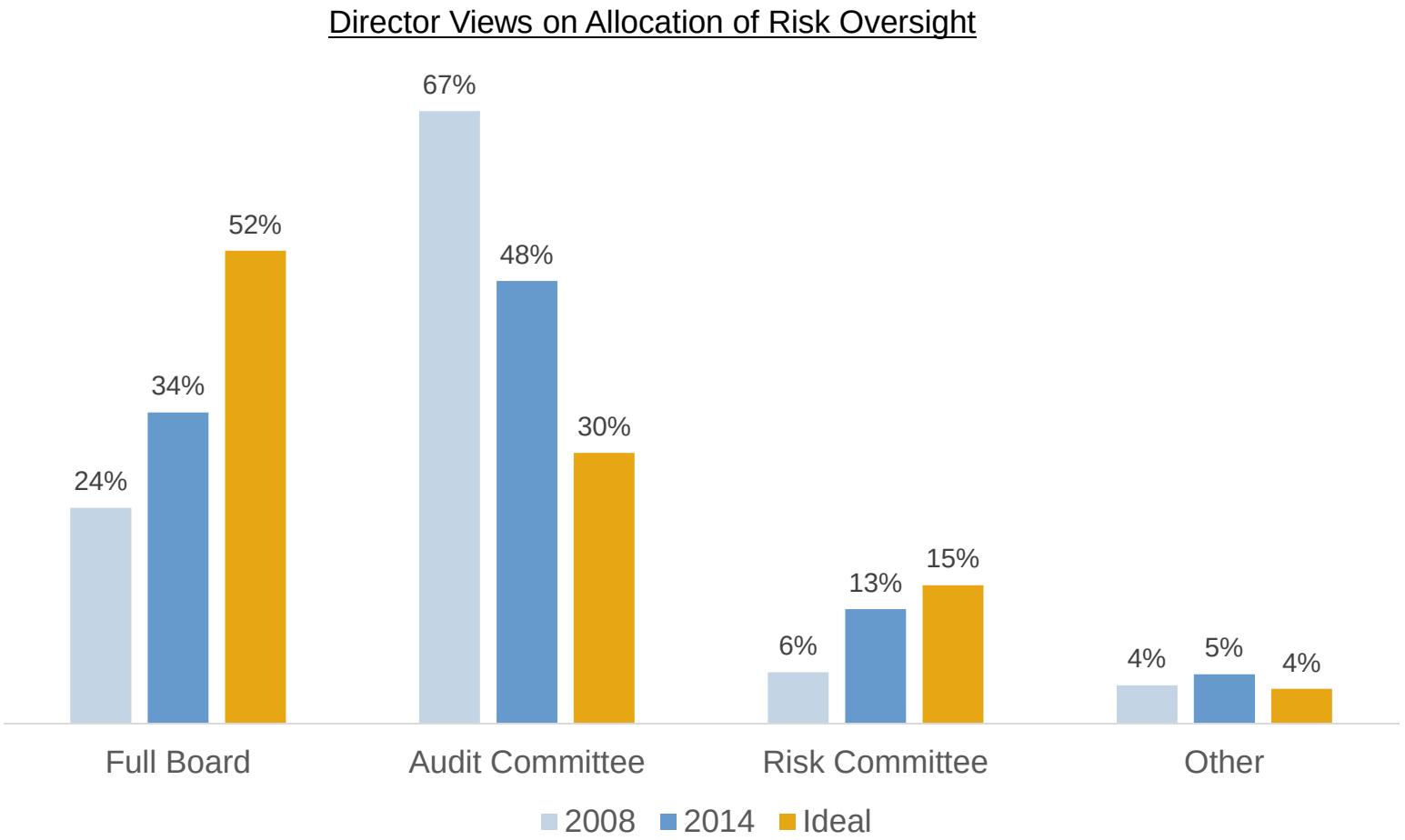
Cyber Security & Changing Board Oversight Responsibilities

May 27, 2015

RUSSELL REYNOLDS ASSOCIATES

Changing Nature of Risk Oversight for Boards

Audit committees are no longer the dominant mechanism for boards to consider all risks, as more directors today recognize risk as a full board responsibility and Risk Committees are on the rise

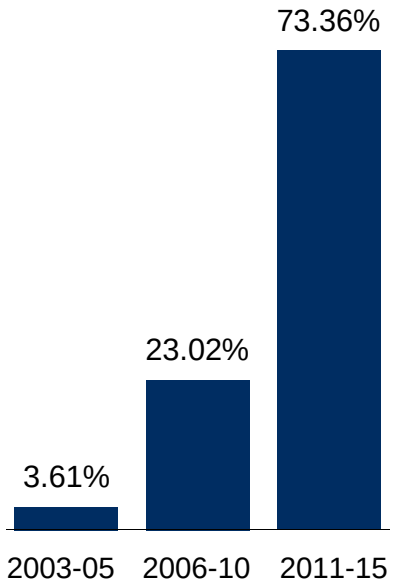


Source: BoardEx RCM, RRA Analysis
2014-2015 Public Company Governance Survey, NACD

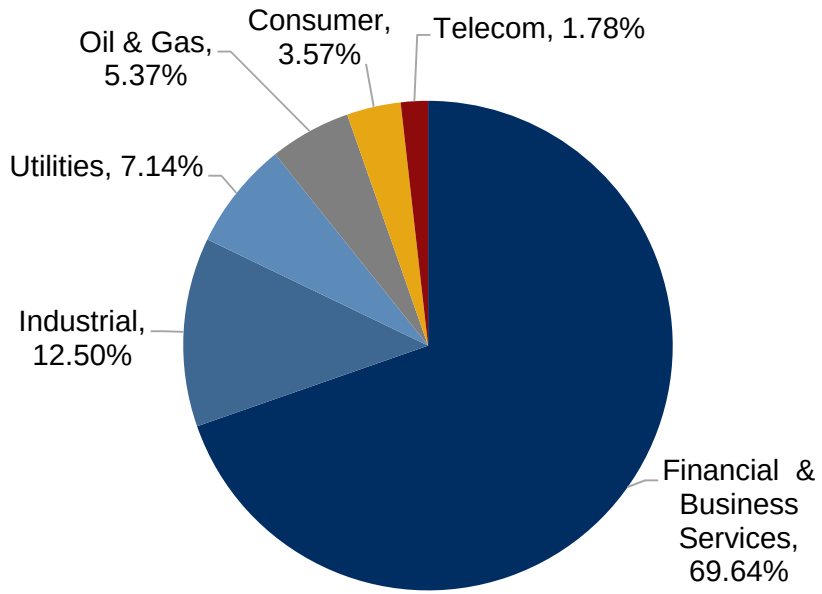
Financial Focus of Risk Committees

Risk Committees remain the most readily observable proxies for how boards view different types of risks. Although only 11% of firms have risk committees, the pace of committee creation is rising fast. However, the majority of existing risk committees are in the financial sector.

Percentage of Risk Committee Appointments, Fortune 500



F500 Companies with a Risk Committee by Sector

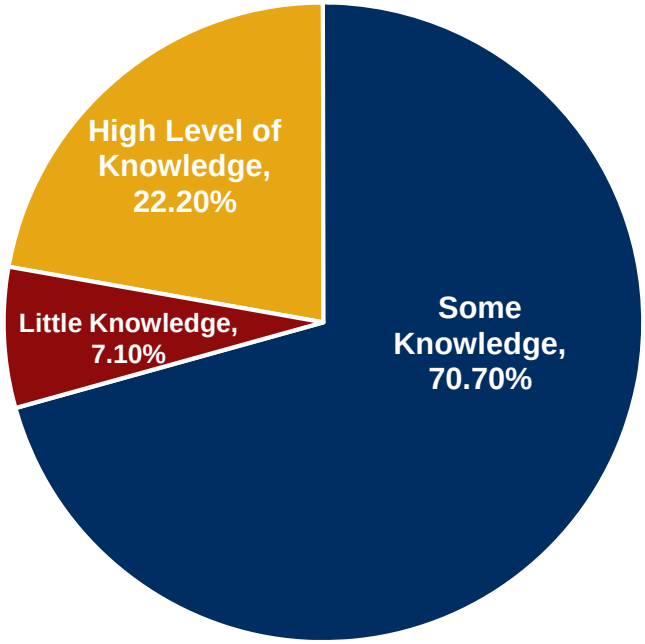


Source: BoardEx RCM, RRA analysis.

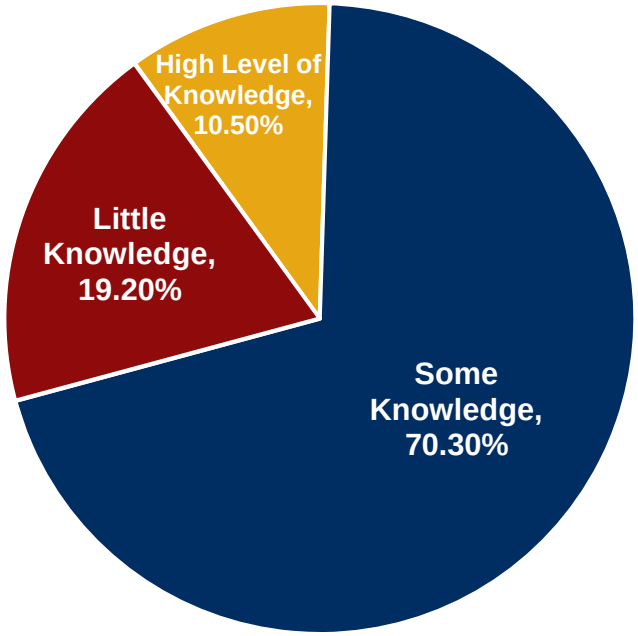
Board Knowledge of Emerging Risks

Despite recent changes in how boards view risk allocation – and additional focus on financial risk - most directors concede lacking knowledge of emerging risks, including cybersecurity.

Directors' Understanding of Emerging & Newly Developing or Rapidly Changing Risks



Director Understanding of Cybersecurity Risks



Source: *2014-2015 Public Company Governance Survey,* NACD

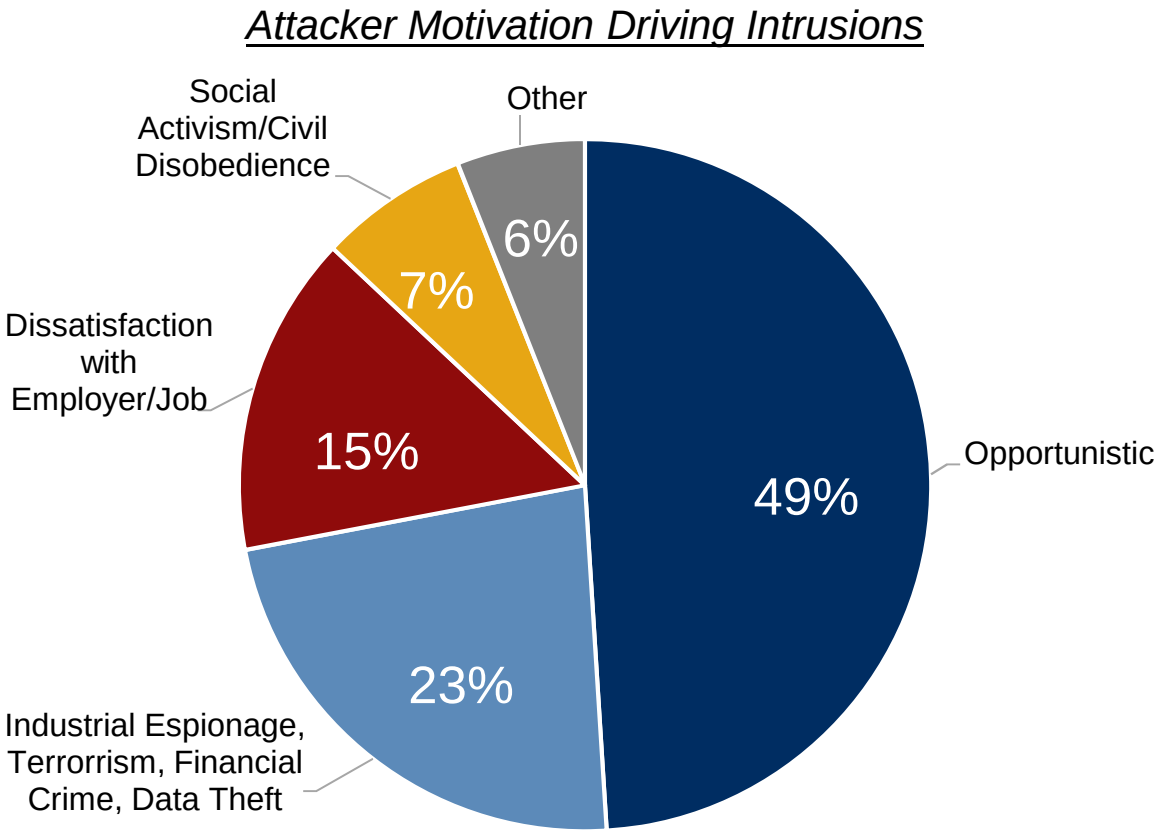
Sophistication of Attacks

Cyber risk is on the rise and evolving with unprecedented sophistication and speed.

More than half **(56%)** of organizations are unlikely to detect a sophisticated cyber breach. **71%** of global cyber compromises go undetected.

The annual cost of cyber breaches to the global economy has reached **$400B**. Between 2009 and 2013, the cost of cyber crime increased by **78%**

One in three organizations around the globe reports being hit by cyber crime. In 2014, **42.8** million breaches were detected, a **48%** leap over 2013.



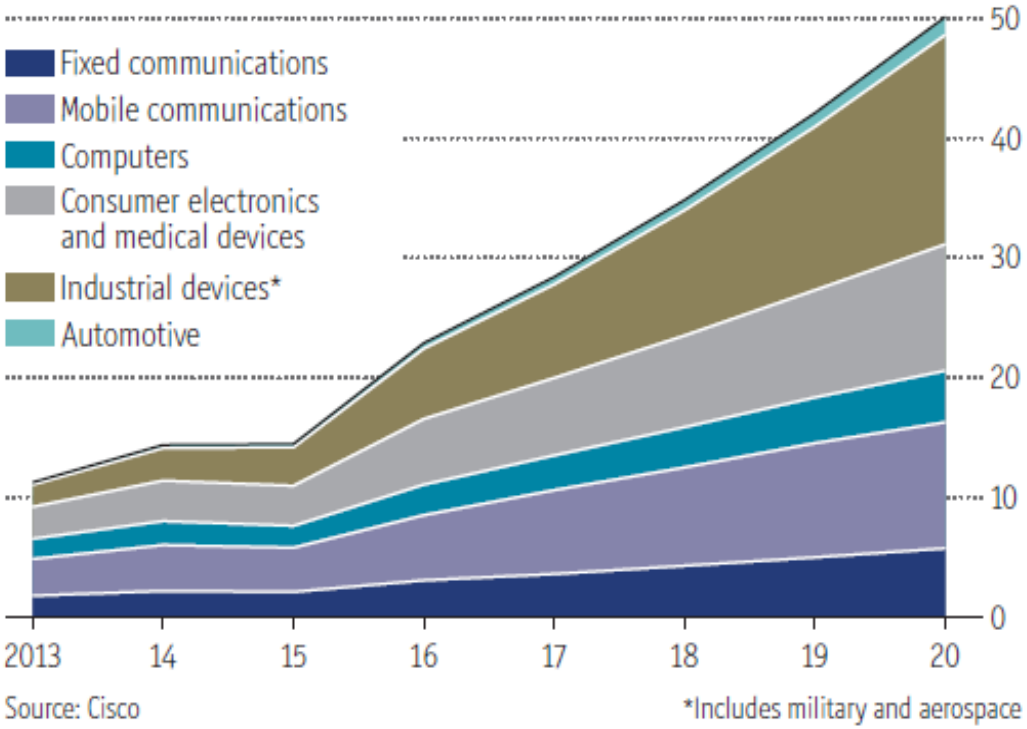
Source: Ernst & Young, *Global Information Security Survey*, 2014;
PwC 18th Annual CEO Survey.
The 2013 IBM Cyber Security Index

Networked Assets Increase Cyber Vulnerability

Companies rely on interconnected networks for an increasing percentage of critical operations, broadening cyber risk potential to many additional industries beyond finance

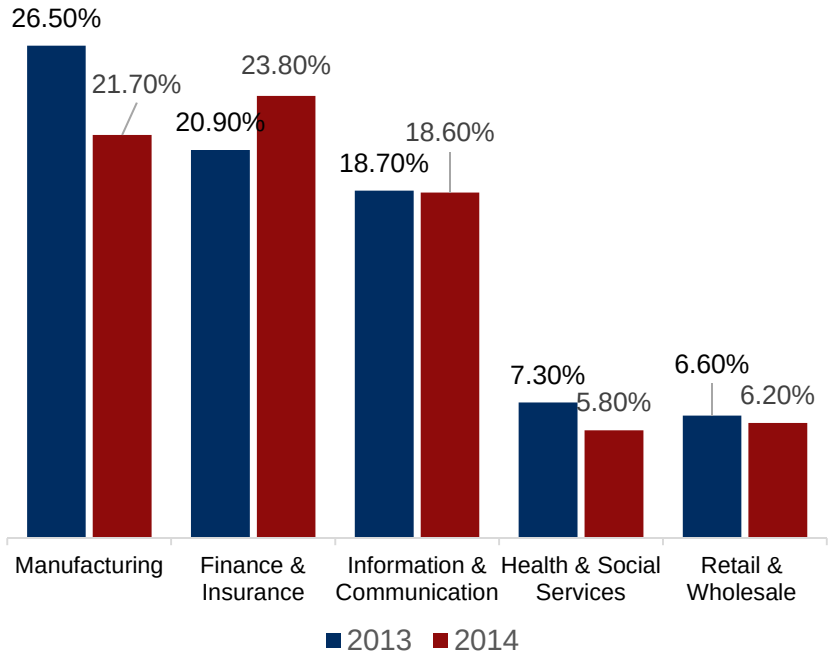
Number of Internet-Connected Devices

Forecasted, Global



Sectors Impacted by Cyber Attacks

2013-2014



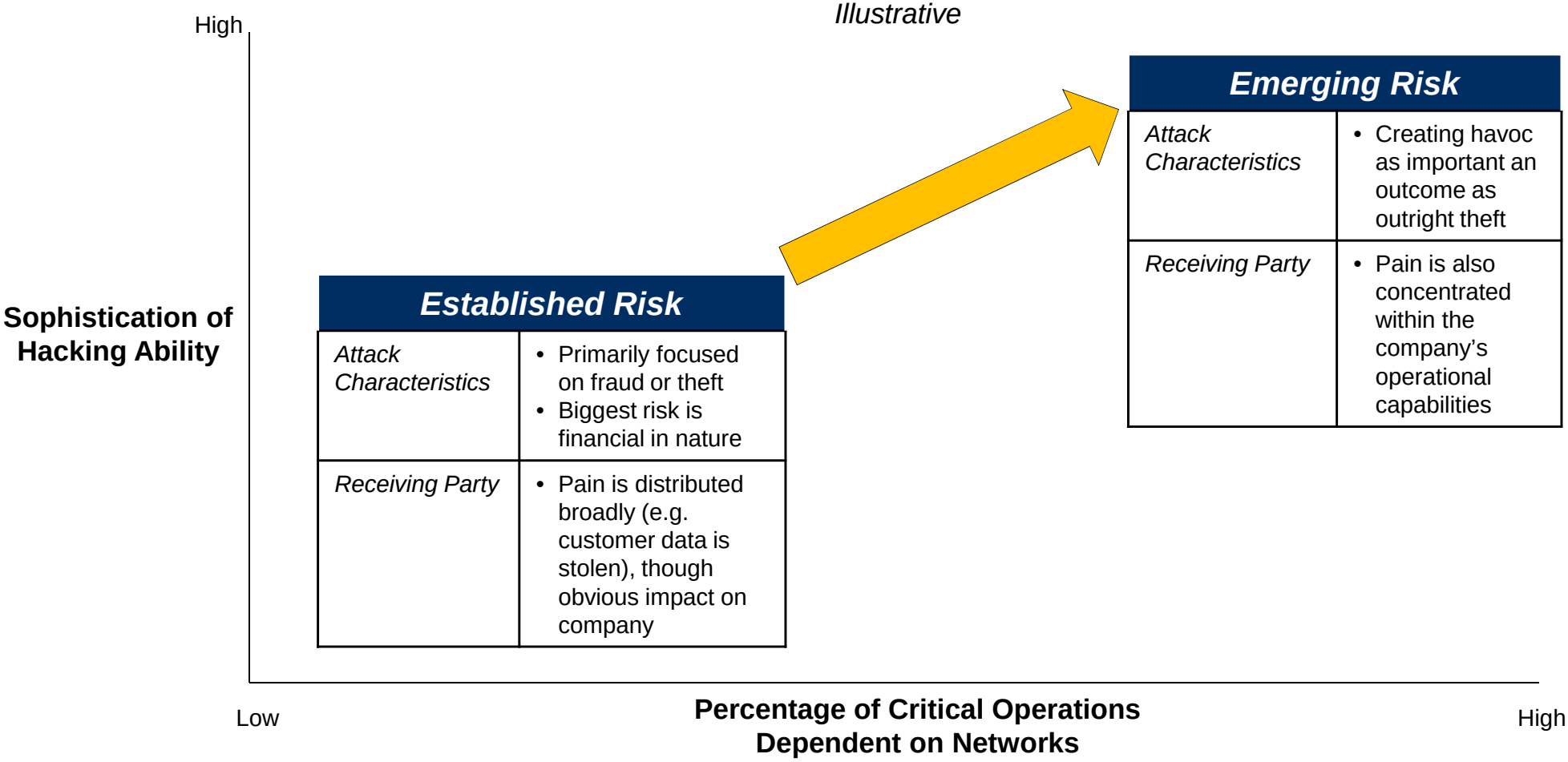
Source: The 2013-2014 IBM Cyber Security Intelligence Index
Special Report on Cyber-Security, The Economist 2014

Not the Attacks of Old

As both hacker sophistication and dependency on networked assets rise at rapid rates, companies face changing cyber-related risks, forcing boards to consider impact on overall risk portfolio

Evolution of Cyber Attacks

Illustrative



Established Risk	
Attack Characteristics	• Primarily focused on fraud or theft • Biggest risk is financial in nature
Receiving Party	• Pain is distributed broadly (e.g. customer data is stolen), though obvious impact on company

Emerging Risk	
Attack Characteristics	• Creating havoc as important an outcome as outright theft
Receiving Party	• Pain is also concentrated within the company's operational capabilities

Source: RRA analysis.

Cost of Cyber Breaches

Cyber attacks on all facets of operations impact companies all over the industry spectrum

Company	Cyber Breach	Aftermath Costs
Booz | Allen | Hamilton	Edward Snowden, a Booz Allen contractor, breached the professional services' company security system and publically disclosed of confidential information about the U.S. government.	Booz Allen has cost in a decline in profit and the trimming of hundreds of jobs.
Aramco	DDOS attackers employed a virus that infected hard drives of over 30,000 Saudi Aramco computers overwriting and effectively destroying data.	The operation of the 30,000 facilities were halted for 10 days due to the cyber breach.
	In 2013, hackers have breached the personal and payment information of about 70 million to 110 million of Target customers.	Customers have sued Target and in the aftermath the court has settled that Target has to pay $10,000 in reparations to each costumer.
The Home Depot	Home Depot was exposed to a cyber breach over a period of five months that went undetected. The company confirmed that 56 million of costumer cards have been compromised.	The company estimated that the investigation, credit monitoring services, call center staffing for affected customers, and other restoration projects would cost about $60 million.
JPMorganChase	In 2014 hackers have configurated employee logins and have accessed more than 90 servers before being caught. The cyber breach exposed some 83 million households and small businesses.	Although, no costumer data was stolen, in the aftermath of the breach, JP Morgan had to invest about $250 million a year on its security system.
Sony Pictures	In 2014 Sony Pictures has suffered cyber breach that has exposed confidential thousands of files and emails of about 6,000 of Sony employees.	The hack caused the shutdown of Sony's computer system for a day and prevented the release of *The Interview*.
Adobe	In 2013, hackers breached more than 38 million of Adobe customer accounts as well as the credit card information of over 3 million customers.	As a consequences, Adobe suffered systemic restoration costs as well as multiple law suits initiated by dissatisfied customers.

Cost of Cyber Breaches, continued

Cyber attacks on all facets of operations impact companies all over the industry spectrum

Company	Cyber Breach	Aftermath Costs
	In 2014, the email service for 273 million users was reportedly hacked.	Yahoo increased its cyber security budget.
	In 2014, eBay suffered multiple cyber breaches that compromised employee logins and disclosed the accounts of 233 million of eBay users.	The hack affected eBay's commerce volume and place on the market. The company had to replace its security system.
	After a cyber breach in 2014, the debit card information from 395 Dairy Queen International and Orange Julius stores was compromised.	The company underwent massive costs by offering free identity repair services for one year to customers in the U.S.
	USIS suffered a cyber breach in August 2014, which led to the theft of employee personnel information.	The U.S. government has suspended most of its work with USIS in the aftermath of the state sponsored cyber breach.
	CHS suffered a cyber breach from April to June 2014 without being detected. As a consequence, the personal data of 4.5 million patients was compromised.	CHS has to change its security system and participate in a federal investigation of the breach.
	Between January and August of 2014, customer information from more than 60 UPS stores, a service provider, was compromised, including financial data.	UPS slashed its full year profit outlook due to loss of customer confidence.
	The U.S. Transportation Command's contractors were successfully breached 50 times between June 2012 and May 2013.	Congress passed new regulations and reporting guidelines for defense contractors that complicated their day to day operations.

Regulatory Measures on Cyber Security

The pace of regulatory action is increasing. Some boards are looking to get ahead of any government mandates by re-thinking how to manage cyber risks today.

2011	In 2011 the SEC has established the Corporate Finance Disclosure Guidance obligating companies to disclose cybersecurity risks and incidents.
2013	The National Institutes of Standards and Technology (NIST) Framework on "Improving Critical Infrastructure Cybersecurity" has offered guidance for boards since 2013
2014	In 2014, the SEC hosted a roundtable, the Conference on Cyber Risks and the Boardroom
2014	Since April 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") conducted cybersecurity preparedness examination. The SEC issued the Cybersecurity examination Sweep Summary in 2015 with suggestions for companies on how to best approach cyber preparedness.
2015	In February 2015, the OCIE has published its report "Cybersecurity Examination Sweep Summary" on the results of its previous investigations. The report had further suggestion on how to mitigate cyber risk and the SEC has promised more regulations to come.

Source: The Office of Compliance Inspections and Examinations ("OCIE")

Key Considerations

For discussion

1. Is cyber security a Board duty?
2. Does amount of exposed infrastructure change how you consider risk?
3. What happens if you wait for government to mandate requirements?
4. Have you considered this cyber risk when screening new directors? If not, why not?
5. How are you measuring cyber risk?
6. Are you adapting to change?
7. Is risk mitigation a priority for your board? Do you have a risk committee? If not, who is in charge of risk oversight on your board?

Summary

Key Takeaways

- Growing importance and regulatory attention to this topic in conjunction with increasing frequency of cyber attacks
- Increasingly important element of Board's expanded risk management responsibility; compliance requirements are being strengthened, especially for select industries with special ties to infrastructure
- Growing disclosure implications tied to materiality
- Among potential action steps that may be required – dedicated Committee focus; vendor assessment; scenario planning/attack response plan; D&O insurance review
- Lack of IT experience in the boardroom has become a challenge to information systems risk management and governance
- Anticipate regular reviews of organization structure and risk management programs; more hands-on checks and balances to challenge executive strategy and preparedness

Requires development of cyber plan, director literacy and use of independent advisors