RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Risk & Responsibility in a Hyper-Connected World: Implications for Enterprises

SESSION ID: PNG-F02

James Kaplan

Chris Rezek

McKinsey&Company

Overview

- Despite years of effort, and tens of billions of dollars spent annually, the global economy is still not sufficiently protected against cyber-attacks -- and it is getting worse; the risk of cyber-attacks could **materially slow the pace of technology and business innovation** with as much as US$3 trillion in aggregate impact.

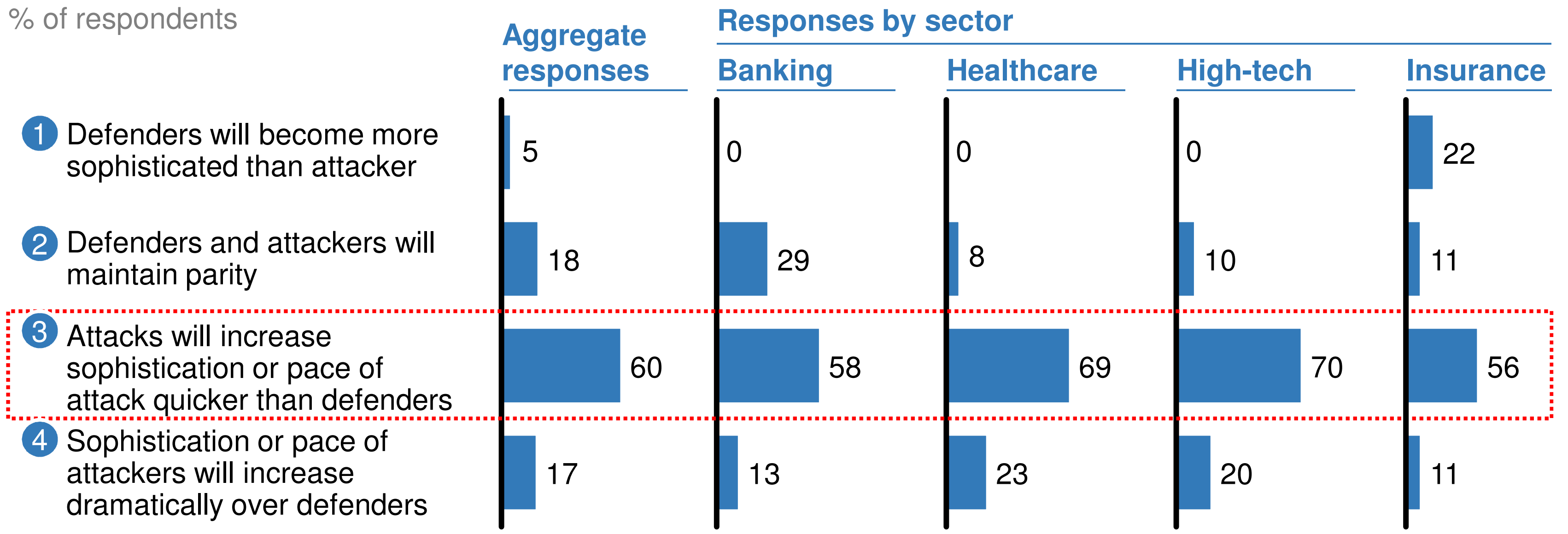
- Enterprise-technology executives agree on the **seven practices they must put in place to improve their resilience in the face of cyber-attacks**; even so, most technology executives gave their institutions low scores in making the required changes

- Given the cross-functional, high stakes nature of cyber-security, it is a **CEO-level issue**, and progress toward cyber-resiliency can only be achieved with active engagement from the senior-most members of the management team

Large majority of technology executives believe that attackers will continue to increase their lead over defenders

⬚ Most frequent response

Interview question: How do you believe the relative level of sophistication will evolve for your institution compared to potential attackers over the course of the next 5 years?



% of respondents

	Aggregate responses	Responses by sector Banking	 Healthcare	 High-tech	 Insurance
1 Defenders will become more sophisticated than attacker	5	0	0	0	22
2 Defenders and attackers will maintain parity	18	29	8	10	11
3 Attacks will increase sophistication or pace of attack quicker than defenders	60	58	69	70	56
4 Sophistication or pace of attackers will increase dramatically over defenders	17	13	23	20	11

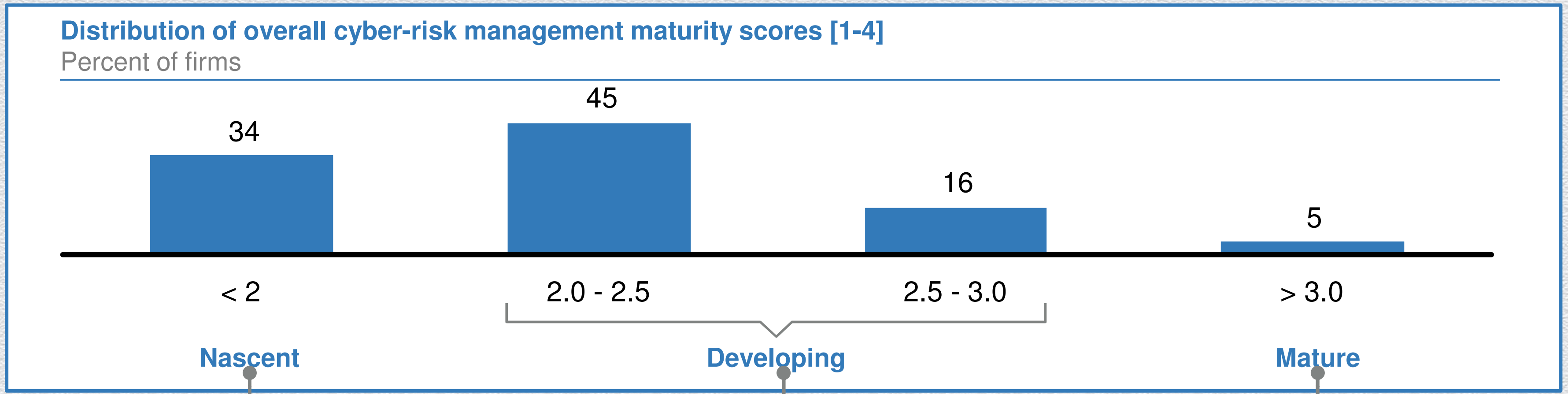
McKinsey&Company

SOURCE: Industry leader interviews; Team analysis

#RSAC

RSACONFERENCE2014

Large majority of firms surveyed had nascent or developing cyber-risk management capabilities



Nascent

- Best effort based evaluation and mitigation of cyber-risks
- No defined single point of accountability nor a clearly defined escalation path to top management

Developing

- Mostly qualitative framework for evaluating and mitigating cyber-risks
- Overall consistent governance model and known single point of accountability in each BU with a defined reporting line to top management

Mature

- Quantitative approach for evaluating and qualitative approach for mitigating cyber-risks
- Defined cyber-security governance model with a single point of accountability within a BU that owns the risks and decision-making

McKinsey&Company

SOURCE: McKinsey Cyber-risk Maturity Survey (CRMS)

What this means in large institutions

<15%

… provide the CISOs with **veto power over IT projects** that violate security policies

… conduct **cyber-security simulations or war games** more than once each year

… evaluate and prioritize **risks related to cyber-attacks** more than once each year

<20%

… include the cyber-security organization’s **impact on business agility** in annual performance evaluations

… include the cyber-security organization’s **impact of broader technology costs** in annual performance evaluations

… ensure the Board has reviewed and approved the **enterprise cyber security strategy**

<35%

… provide the time for the CISOs to **meet regularly with the CEO**

… communicate a list of **business assets that are most critical to protect** to the Board

… analyze all **major attempted or successful attacks**

<55%

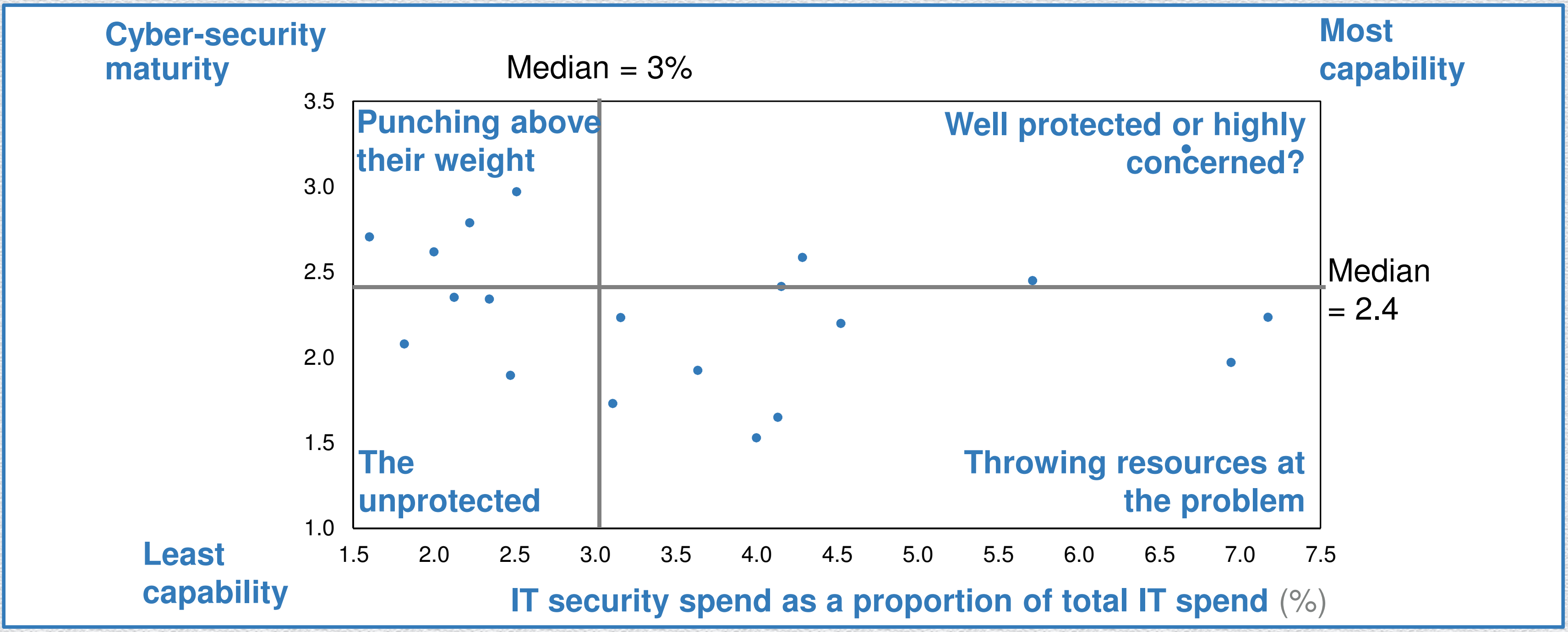
… conduct systematic **penetration testing**

… define **minimum standards for data protection** for sensitive information

… update **intelligence about attackers** more frequently than once a year

SOURCE: McKinsey Cyber-risk Maturity Survey (CRMS)

High expenditures do not necessarily yield sophisticated capabilities; many firms are 'throwing money at the problem'



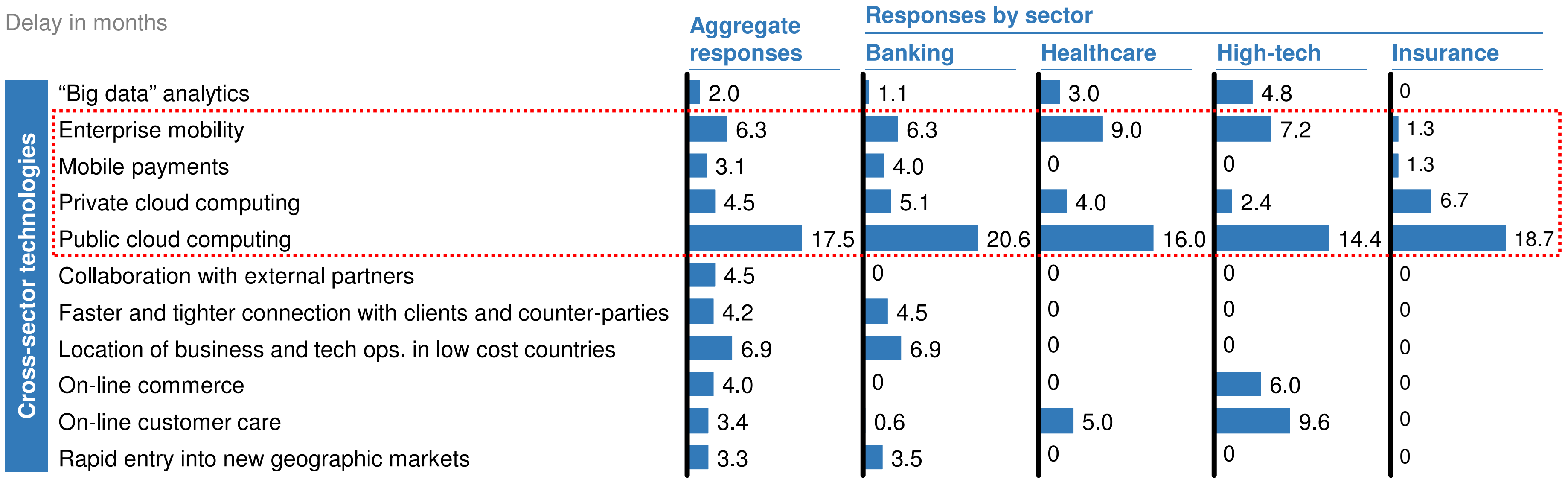
McKinsey&Company

SOURCE: McKinsey Cyber-risk Maturity Survey (CRMS)

Concerns about cyber-attacks have slow deployment of cloud and mobile capabilities

⬚ Most frequent responses

Interview question: What is the likelihood that concerns about cyber-attacks will slow the adoption of the following business and technology innovations for your institution?



Delay in months

Cross-sector technologies	Aggregate responses	Responses by sector: Banking	Healthcare	High-tech	Insurance
"Big data" analytics	2.0	1.1	3.0	4.8	0
Enterprise mobility	6.3	6.3	9.0	7.2	1.3
Mobile payments	3.1	4.0	0	0	1.3
Private cloud computing	4.5	5.1	4.0	2.4	6.7
Public cloud computing	17.5	20.6	16.0	14.4	18.7
Collaboration with external partners	4.5	0	0	0	0
Faster and tighter connection with clients and counter-parties	4.2	4.5	0	0	0
Location of business and tech ops. in low cost countries	6.9	6.9	0	0	0
On-line commerce	4.0	0	0	6.0	0
On-line customer care	3.4	0.6	5.0	9.6	0
Rapid entry into new geographic markets	3.3	3.5	0	0	0

Note Data is shown for technologies chosen by more than three respondents
Top 6 technologies are also classified under High-tech

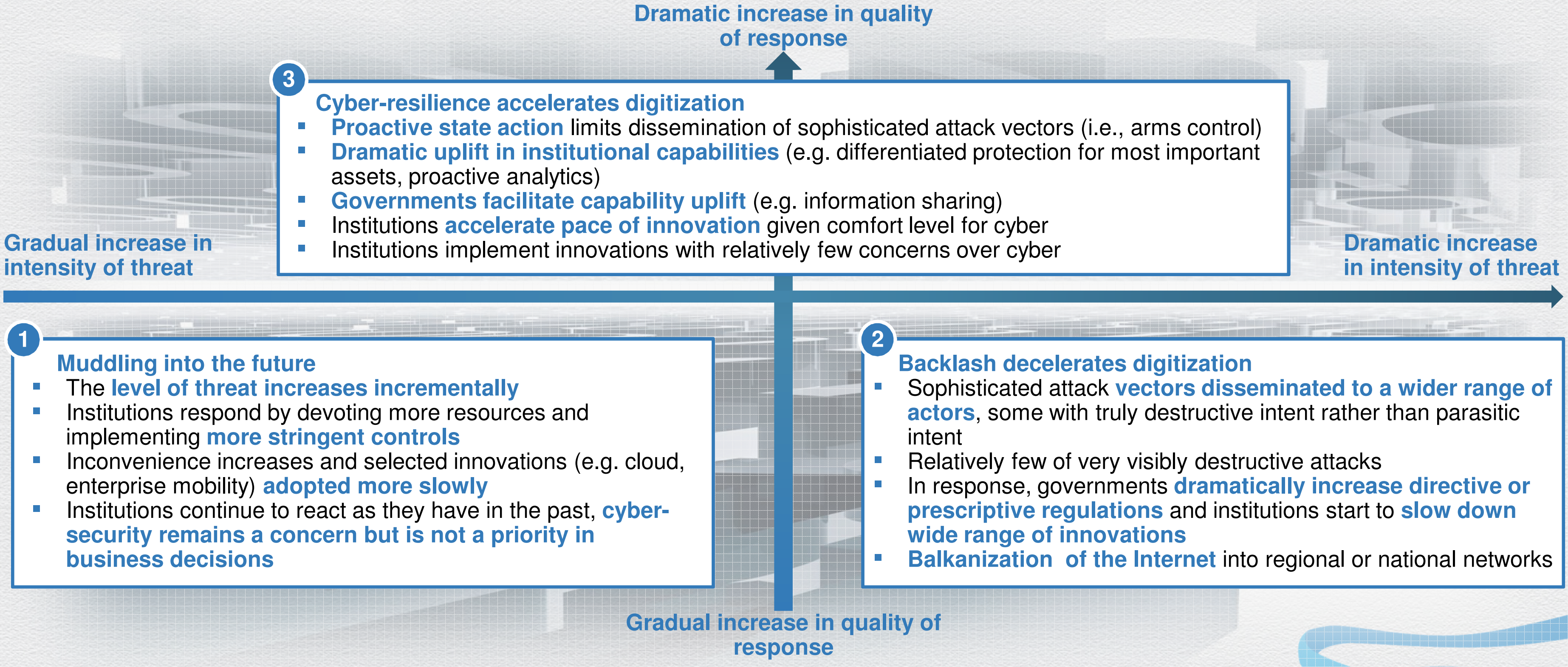
SOURCE: Industry leader interviews; Team analysis

McKinsey&Company

#RSAC

RSACONFERENCE2014

Alternative future scenarios for 2020 highlight risk of a regulatory, consumer and institutional backlash against digitization



Dramatic increase in quality of response

Gradual increase in intensity of threat

Dramatic increase in intensity of threat

Gradual increase in quality of response

3 **Cyber-resilience accelerates digitization**

- **Proactive state action** limits dissemination of sophisticated attack vectors (i.e., arms control)
- **Dramatic uplift in institutional capabilities** (e.g. differentiated protection for most important assets, proactive analytics)
- **Governments facilitate capability uplift** (e.g. information sharing)
- Institutions **accelerate pace of innovation** given comfort level for cyber
- Institutions implement innovations with relatively few concerns over cyber

1 **Muddling into the future**

- The **level of threat increases incrementally**
- Institutions respond by devoting more resources and implementing **more stringent controls**
- Inconvenience increases and selected innovations (e.g. cloud, enterprise mobility) **adopted more slowly**
- Institutions continue to react as they have in the past, **cyber-security remains a concern but is not a priority in business decisions**

2 **Backlash decelerates digitization**

- Sophisticated attack **vectors disseminated to a wider range of actors**, some with truly destructive intent rather than parasitic intent
- Relatively few of very visibly destructive attacks
- In response, governments **dramatically increase directive or prescriptive regulations** and institutions start to **slow down wide range of innovations**
- **Balkanization of the Internet** into regional or national networks

McKinsey&Company

SOURCE: Industry leader interviews; Team analysis

Potential impact of cyber security risks to global economy could be as much as $3 trillion

⬚ Impacted by cyber security risks

US$ Billion	Est. value created by 2020		Impact of alternative future scenarios		
Business & technology innovation total	**Low**	**High**	**1. Muddling**	**2. Backlash**	**3. Resilience**
▪ Cloud technology	1020	2700[2]	(130)-(470)[4]	(390)-(1,410)[4]	-
▪ Internet of things	1600	2150[2]	(90)-(210)	(270)-(630)	-
▪ Mobile internet	1330	1550[2]	(70)-(150)	(210)-(450)	-
▪ Rapid entry into new markets	170	50[1]	(10)	(20)-(40)	-
▪ Automation of knowledge work	2500	720[2]	(80)-(100)	(240)-(310)	-
▪ Social technologies	750	350[3]	(20)-(30)	(70)-(100)	-
▪ E-commerce	270	240[1]	(10)	(20)-(40)	-
▪ Autonomous and near-autonomous vehicles	120	1020[2]	(20)	(10)-(70)	-
▪ Next-generation genomics	420	540[2]	(10)	(20)-(40)	-
▪ Others	1460	2700[2]	-	-	-
Total	9,630	21,630	(410)-(1,020)	(1,230)-(3,060)	-

[1] Estimate does not include consumer surplus; based on IMF: April 2013 WEO data & MGI Internet Matters report; May 2011

[2] Based on MGI Disruptive Technologies projections for 2025 assuming linear ramp-up from mid-2013 to 2025 and scaling back to 2020

[3] Based on MGI Social Economy projections for mid-2012, extrapolated to 2020 based on 10-year average world GDP growth rate 2.6%

[4] >80% of impact for cloud is due to delayed adoption of public cloud

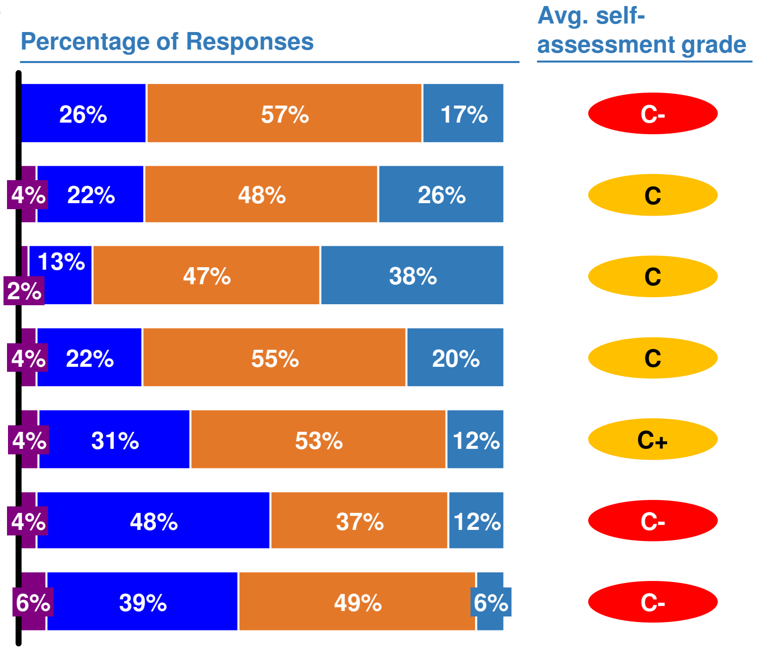
McKinsey&Company

Most technology executives gave their institutions low scores in making the required changes so far

What actions that your institution could take would have the most impact in reducing the risk associated with cyber-attacks? (%)

■ No/Limited impact ■ Moderate Impact ■ Significant Impact ■ Game changer

1. Prioritize information assets and related risks in a way that helps engage business leaders
2. Provide differentiated protection for most important assets
3. Develop deep integration of security into the technology environment to drive scalability
4. Deploy active defenses to be proactive in uncovering attacks early
5. Realistic testing to improve incident response
6. Enlist front-line personnel – helping them understand value of information assets
7. Integrate cyber-resilience into enterprise-wide risk management and governance processes



McKinsey&Company

#RSAC

RSACONFERENCE2014

1 Prioritize information assets and related risks in a way that helps engage business leaders

DISGUISED EXAMPLE

Plotting risk likelihood against impact helps focus investment `

Impact

- Catastrophic impact & reputational consequences
- Includes production loss and damage to facilities
- Economic loss >$1B
- Economic loss $100M-$1B
- Some reputational impact and/ or limited reputational consequences
- Economic loss <$100 million

Impact	Low	Medium	High
High	🟧 g d	🟥 b	🟫 j
Medium	🟨 f a	🟧 e c	🟥 i
Low	🟩 h	🟨	🟧 k

Low
- Few highly motivated actors None are sophisticated
- Complex attacks required

Medium
- Actors with high motivation/ incentives are not sophisticated
- Attacks required are moderately complex

High
- Sophisticated actor(s) with high motivation/ incentives
- Attacks required are low complexity

Likelihood

Risks

- **a** Competitor steals algorithm used in highly successful foreign exchange trading operating
- **b** Potential JV partner in emerging market gets access to negotiating strategy
- **c** System administrator accesses M&A information and trades ahead of announcement
- **d** Customer account information released publically on the internet
- **e** Leakage of internal email communications (e.g., email) among senior executives about decisions related mortgage re-financing
- **f** One day outage of online channel for customers to access and manage bank accounts in core markets
- **g** One hour outage in credit card authorization network
- **h** Half-day interruption in remote access services
- **i** Retail customers credit card accounts hijacked and used for fraudulent payments
- **j** High net worth customer brokerage accounts targeted by sophisticated attacks
- **k** Programmer inserts code diverting large number of small amounts

McKinsey&Company

#RSAC

RSA CONFERENCE 2014

4 Deploy active defenses to uncover attacks proactively the emerging model looks like

From…	…to
i **A reactive cyber intelligence and defense model based on alerting and response,** which tends to be focused on the “last event” or generic solutions, not the latest headlines	▪ **A proactive cyber intelligence model based on dynamic intelligence and analytics** to learn, anticipate, and prioritize actions. Ensuring preparation for the next attack by mapping out the ‘anatomy’ of the highest risk scenarios, ensuring complete visibility over these assets, and arranging third-party contracts in advance
ii **Cyber intelligence reports are not often used to influence business decisions,** because they do not provide the right call to action for the business	▪ **Cyber intelligence which is business-relevant,** based upon understanding the main elements of cyber value creation and business risk priorities ▪ **Continuous improvement should be at core of the process** in order to learn, adapt, and improve the impact of intelligence products upon decision makers/business leaders
iii **Detection of threats is manual and time-consuming**, with security personnel focusing their time on assessing current threats and reacting to events in real-time	▪ Achieving effectiveness and efficiency with **a deliberate division of labor between man and machine, by automating or outsourcing certain functions** so that security personnel can focus on the most complex tasks where judgment is necessary, at either end of the lifecycle
iv **Intelligence gathering and threat gathering which is mostly inward looking**, only considering the threats known locally rather than leveraging external contacts and resources	▪ **Source intelligence which is global,** leveraging all internal and external data sources, including advanced threat intelligence and information-sharing in the industry

McKinsey&Company

#RSAC

RSACONFERENCE2014

7 Integrate cyber-resilience into enterprise-wide risk management and governance process

Key contributions by business function

Product development	▪ Incorporate security concerns into product concepts and take security requirements into account in developing business cases
Marketing, sales & customer care	▪ Design programs that encourage appropriate customer behavior (e.g. password strength, not sharing passwords) ▪ Communicate cyber-security related issues in a sensitive fashion
Legal, privacy and regulatory	▪ Provide input on customer privacy priorities ▪ Set policies that strike appropriate balance between customer privacy and organization's need to protect itself ▪ Engage proactively with regulators on cyber-security plans ▪ Shape the external regulatory and public policy environment
Procurement	▪ Negotiate security requirements into relevant vendor contracts ▪ Put enforcement mechanisms in place
Human resources	▪ Set policies that strike appropriate balance between employee privacy and organization's need to protect itself ▪ Drive cultural change and help put targeted training mechanisms in place
Operations	▪ Take implications about data protection into account when making site decisions ▪ Reinforce policies about data usage and protection
Risk management	▪ Incorporate cyber-security risks into enterprise-wide risk management decision-making and reporting mechanisms

Perspective on regulation depends on sector, with banking most skeptical; health care believes it could drive management attention

⬚ Most frequent response by executives from all sectors except healthcare & insurance

Interview question: What impact does government regulation have on your ability to manage cyber-security related risks?

% of respondents	Aggregate responses	Responses by sector			
		Banking	Healthcare	High-tech	Insurance
1 No/Limited impact	14	18	0	21	8
2 On balance it encourages us to be more secure in a helpful way	40	25	46	21	67
3 It requires a lot of time and effort, but does not really make us more secure	33	36	38	43	25
4 It makes us less secure by requiring actions that do not make sense or taking resources away from higher priority actions	13	21	15	14	0

McKinsey&Company

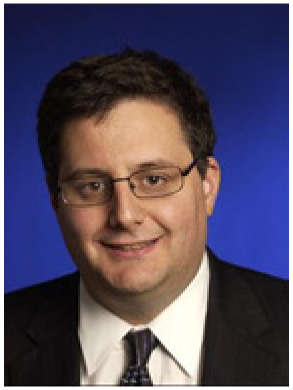
SOURCE: Industry leader interviews; Team analysis

Structural and organizational challenges mean senior management must help drive changes required for cyber-resiliency

Typical challenges	Representative quotes from senior managers
Need to accept risks given competitive imperatives	*"Yes, there may be security concerns about social media, but this is* ***where our customers are*** *and they expect us to interact with them there."*
Tough to quantify "risk" or "risk mitigation"	*"It feels like we're constantly spending more on security, but I have* ***no idea whether that's enough*** *or even what it does"*
Tough to get executive engagement on tradeoffs	*"I get detailed IT security reports, but* ***don't know whether several thousand intrusions detected is good*** *or bad"*
Tough to change behavior at the front lines	*"I have marketing staff and researchers* ***rebelling against security policies*** *that they say prevent them from getting work done"*

Role of senior management in getting the right cyber-security capabilities in place

- Set overall expectations on institutional risk appetite
- Providing input on prioritization of information assets and trade-offs between business protection and operational impacts
- Incorporate cyber-security considerations into product, customer and location decisions
- Sponsor integration of cyber-security policies into other functions (e.g. HR, corporate security, vendor management)
- Drive behavioral changes in senior management team (e.g. for handling sensitive business materials)
- Communicate need for behavioral change at the front line
- Incorporate cyber-security into regulatory and public affairs agenda
- Backstop security team in enforcing important polices
- Get actionable reporting in place for board



James Kaplan

james_kaplan@mckinsey.com

@jmk37

Chris Rezek

chris_rezek@mckinsey.com