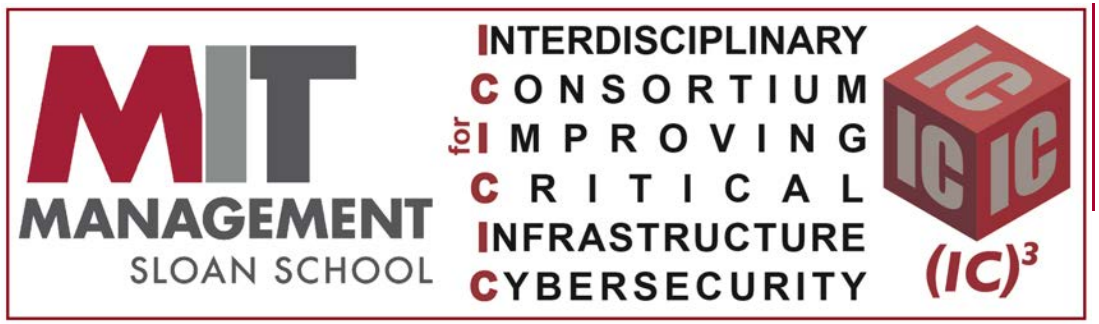


Studying the Tension Between Digital Innovation and Cybersecurity

at *Twenty-third Americas Conference on Information Systems, Boston, August 12, 2017*

Natasha Nelson
Schneider Electric Company
natasha.v.nelson@gmail.com

Stuart Madnick
MIT Sloan School of Management
smadnick@mit.edu

Agenda

- Why is this question important?
- Framework and Hypothesis
- Quantitative Analysis
- Qualitative Analysis
- Conclusions and Recommendations

Economic Impact

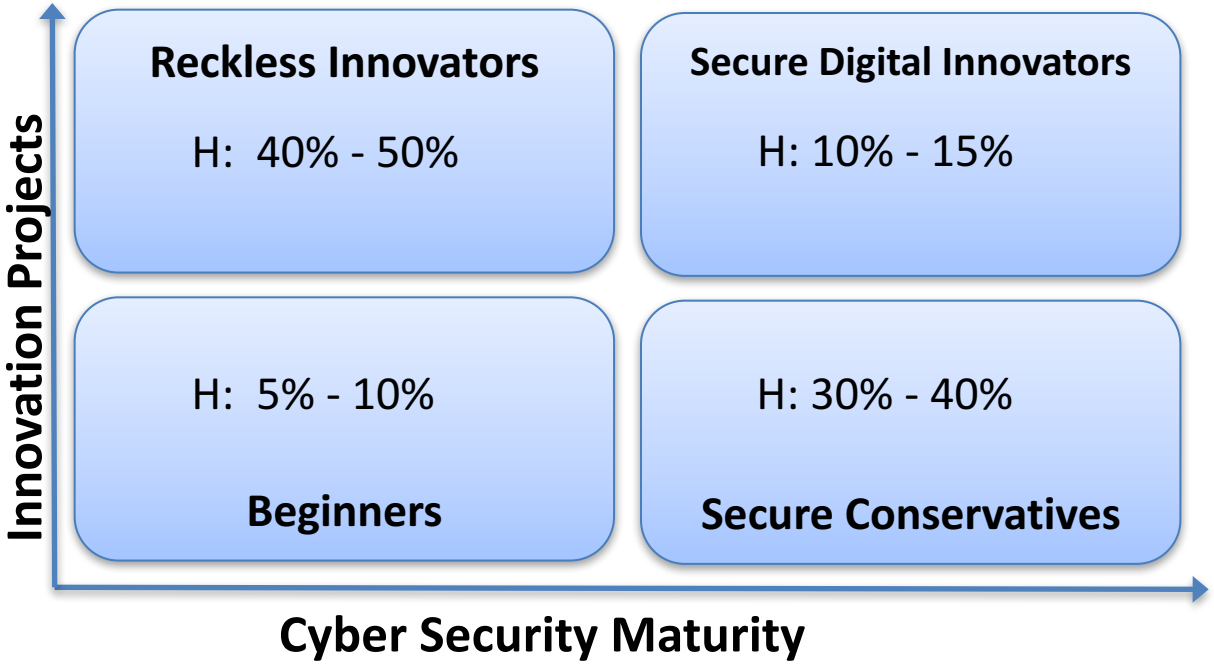
"Only a few CEOs realize that the real cost of cybercrime stems from delayed or lost technological innovation—problems resulting in part from how thoroughly companies are screening technology investments for their potential impact on the cyberrisk profile."

McKinsey / WEF Research, 2014

"Most of the applications used today on the Internet are created by commercial actors whose primary motivation is profitability. …There is a tension between meeting the needs of the user and adding features that make money. The balance of these sorts of issues are often the subject of law and regulation, as well as a changing landscape of norms and expectations."

David D. Clark, The Landscape of Cyber-Security, Dec. 2015

Framework and Hypothesis



- Data required:
  - Innovation metric
  - Proxy for Cyber. Sec. Maturity
  - Impact Measurement
  - Examples / stories

Model improvements:

- Refine category definitions
- Analyze findings
- Examples and stories to support / explain findings
- Discover tensions created
- Identify additional factors

Sources of data

- 54 Survey Reponses

Row Labels	Asia / Pacific	Europe / Middle East / Africa	Latin America / Caribbean	North America	Grand Total
Board Member	1	1		2	4
CEO	2	1		3	6
CFO			2		2
CIO	1	4		7	12
CISO				2	2
IT Director / Manager	5	1		5	11
Marketing Executive	3				3
Operations Executive		1			1
Other	6	2		1	9
VP of IT	3			1	4
Grand Total	21	10	2	21	54

- Plus 14 interviews

Framework and Hypothesis

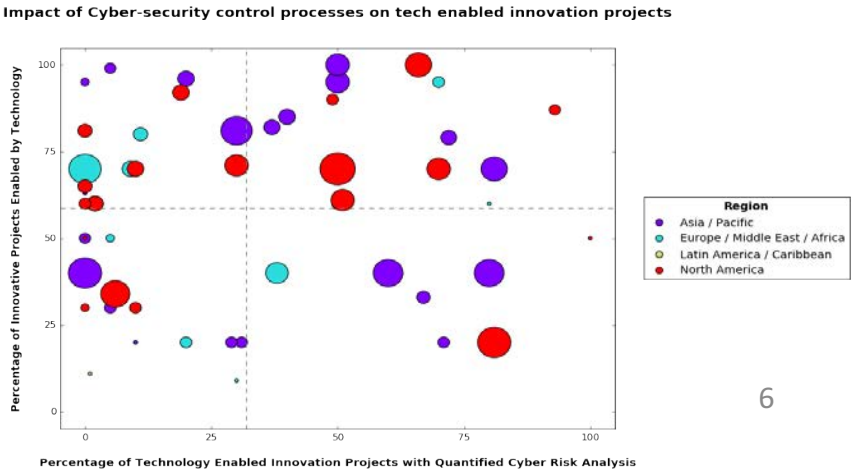
% of Innovation Projects enabled by technology

Reckless Innovators H: 40% - 50% **F: 29.63%**	Secure Digital Innovators H: 10% - 15% **F: 29.63%**
H: 5% - 10% **F: 27.78%** Beginners	H: 30% - 40% **F: 12.96%** Secure Conservatives

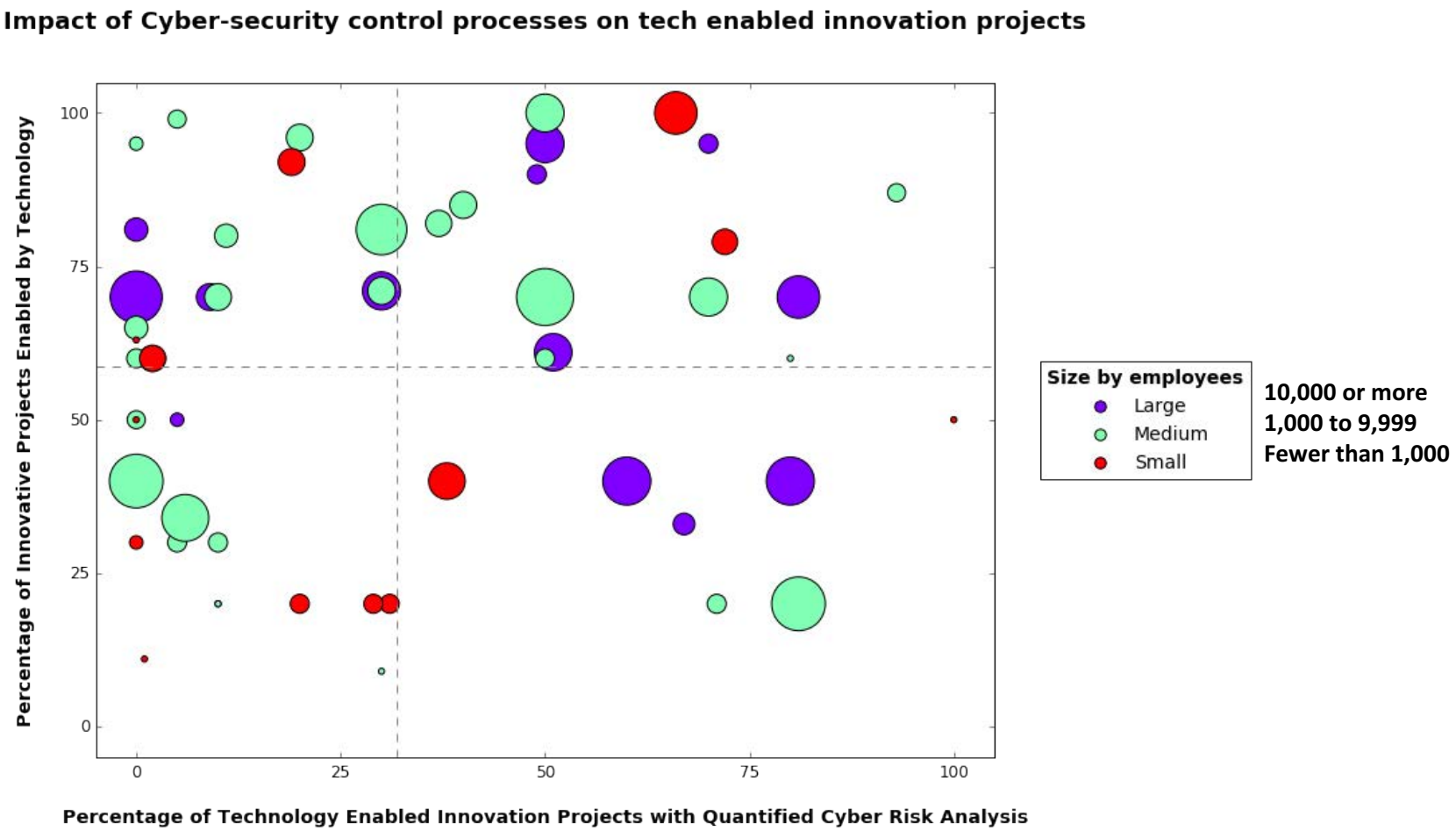
% of Projects with quantified Cyber-risk measurement

H: Original Hypotheses
F: Actual Data Results

New, Refined Model



Analysis by Company Size

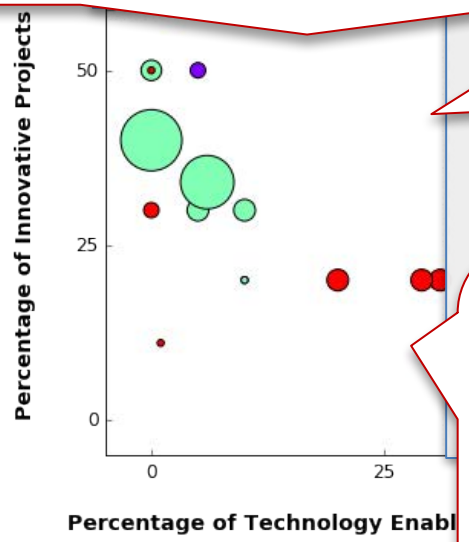


Size of the bubble - % of Projects negatively impacted by cyber-security control process

1st Quadrant

A large global auto-parts manufacturer

"IT maturity is estimated generously at a 2 out of 5. It's a heavily decentralized environment where literally 100+ divisions are able to do their own thing globally with very little governance over IT. As an unintended consequence you get proliferation of technologies and lack of standards. Since there was no IT governance and every location could chose their own platform, implementing security measures was the #1 impairment. Cross-divisional innovations will happen after we establish centralized IT utility and address security."



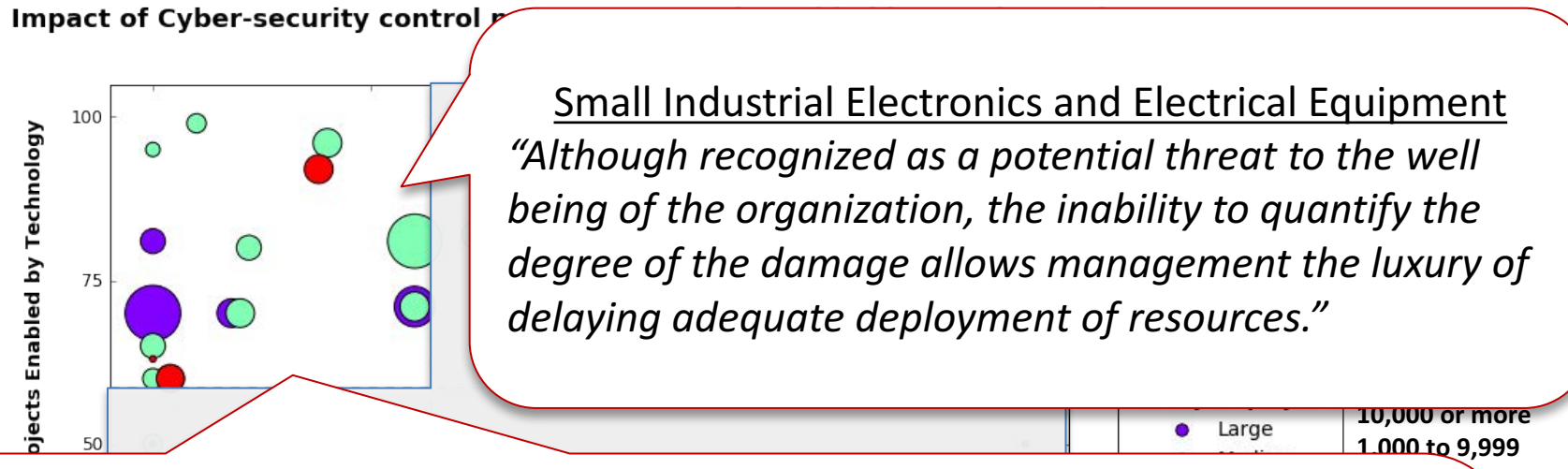
"We are a startup engaging in renewable energy business. At the moment, we spend quite little time on cyber-risk analysis."

VC

"For early stage investors, the Minimum Viable Product needs to be built just to get the system up and running, get the product going; VCs are looking at the team, market and the product, not at the security of the product; security will be looked as part of exist due diligence"

Size of the bubble - % of Projects

2nd Quadrant



Small Industrial Electronics and Electrical Equipment

"Although recognized as a potential threat to the well being of the organization, the inability to quantify the degree of the damage allows management the luxury of delaying adequate deployment of resources."

A large product centric engineering company

"There is support [for cyber-security] from upper management and leadership, but the problem is that it's not trickling down to the project management teams, because they don't have time to code securely. If you are stopping a product release, especially with the timelines, then you are likely to be fired. We need the product to be released fast due to competition.

…Security is very new for this industry. Engineers that have been doing this for 20 years – all of a sudden they need to think of something new, people are used to their own ideas and the process. "

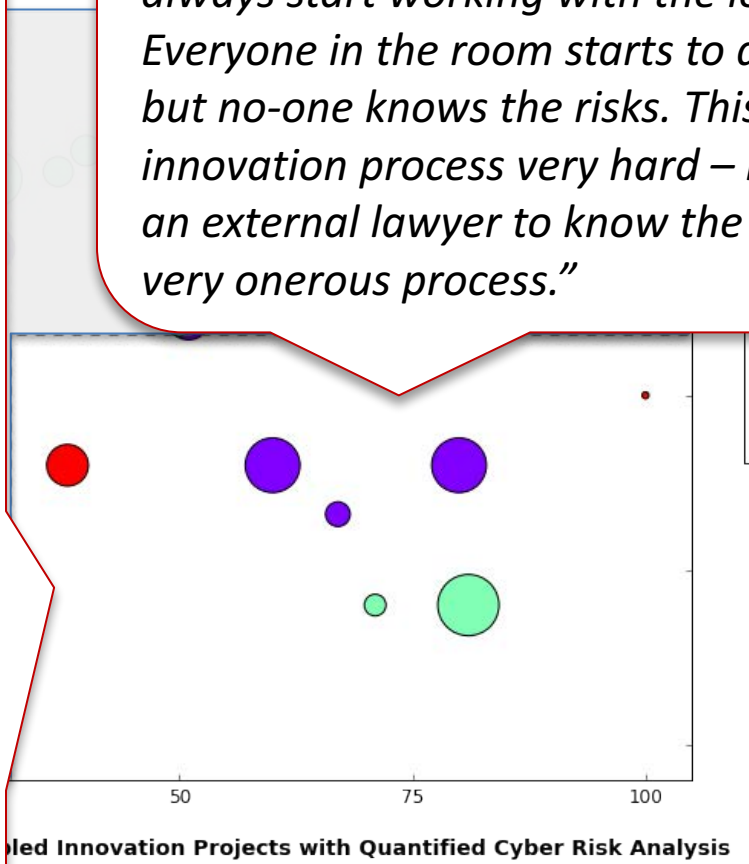
3rd Quadrant

Government contractor

"Poor alignment between field operations and centralized Cyber Security Unit. Also poor digital maturity and risk awareness in senior business leadership. Result: Fairly strict and conservative cyber security policy and practice. Opportunities are lost due to conservative security policies and lack of appetite for more transformative digital development initiatives."

Large transportation company

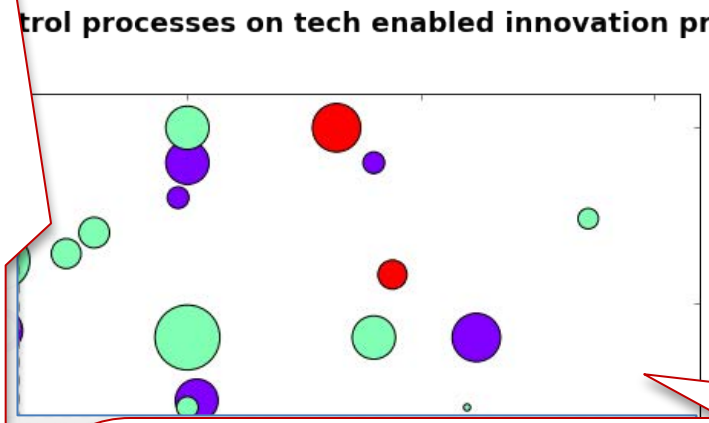
"When we start evaluating a new project, we always start working with the legal issues. Everyone in the room starts to discuss the risks, but no-one knows the risks. This makes the innovation process very hard – it is very hard for an external lawyer to know the business, so it's a very onerous process."



…led Innovation Projects with Quantified Cyber Risk Analysis

…cts negatively impacted by cyber-security control process

4th Quadrant



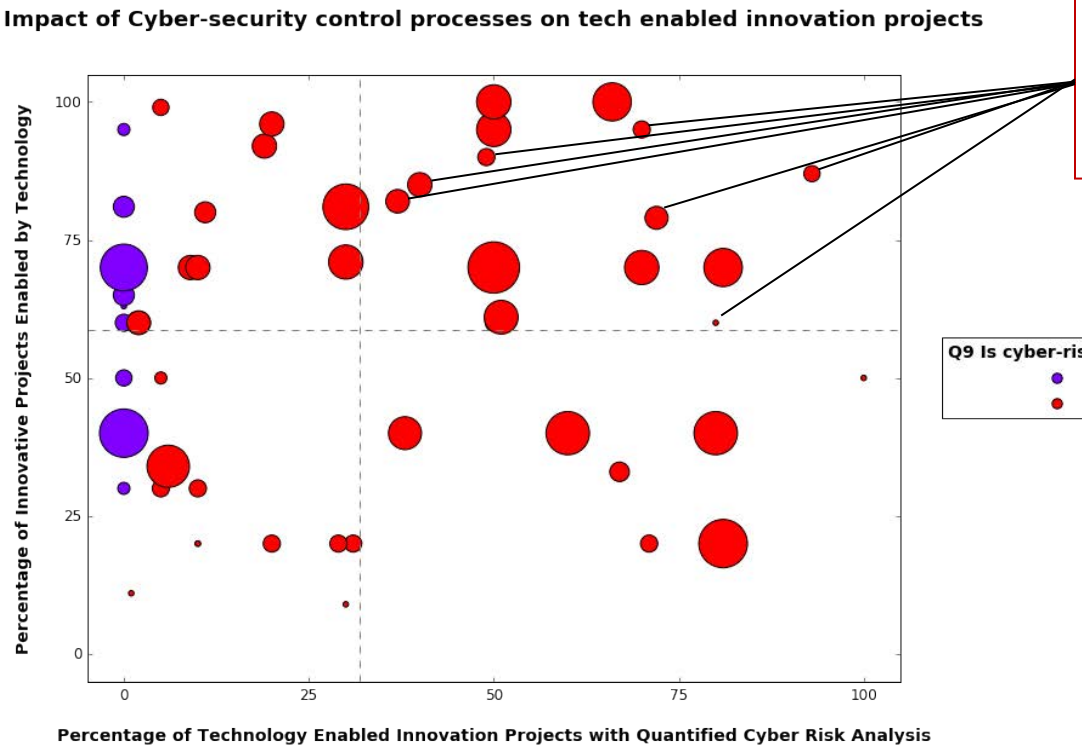
Large Healthcare / Retail Company

"We have PCI and HIPAA regulations. Few years ago we had a breach. There is now a Digital innovation group – a whole new set of processes is being built right now. Our CIO is ruthlessly serious about security and there is a cyber-security strategy. Risk/reward discussions happen all the time. We would prototype with the current technology to do feasibility testing. Our legal, privacy and security teams are highly involved in the process. If we want to build a new technology, then they need to focus on evaluating it."

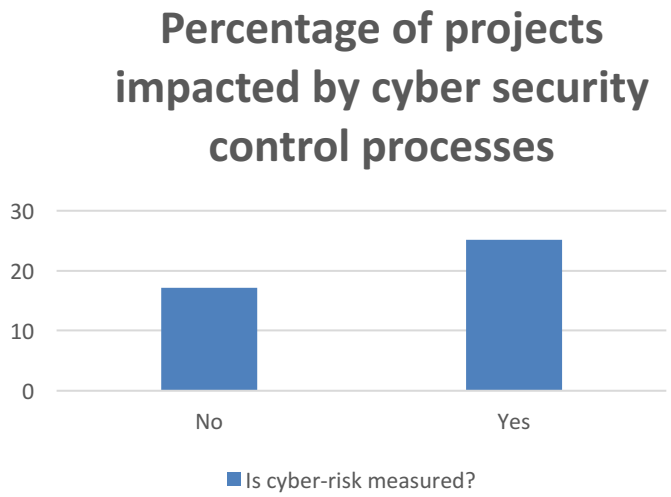
Medium size Marketing Data Analytics Fintech company

"The company is very conservative and cyber-security is an audit committee board level interest. When Target happened and their CEO was fired, our CEO announced that PCI compliance of our product is our #1 priority. People hated it – investment was large and cut-out a huge number of possible projects. Company learned that building security upfront is a lot less expensive, because this PCI project cost them a lot. Today, cyber-security enables innovation. What we need to do better is learn how can cyber-security accelerate innovation."

Analysis by measurement

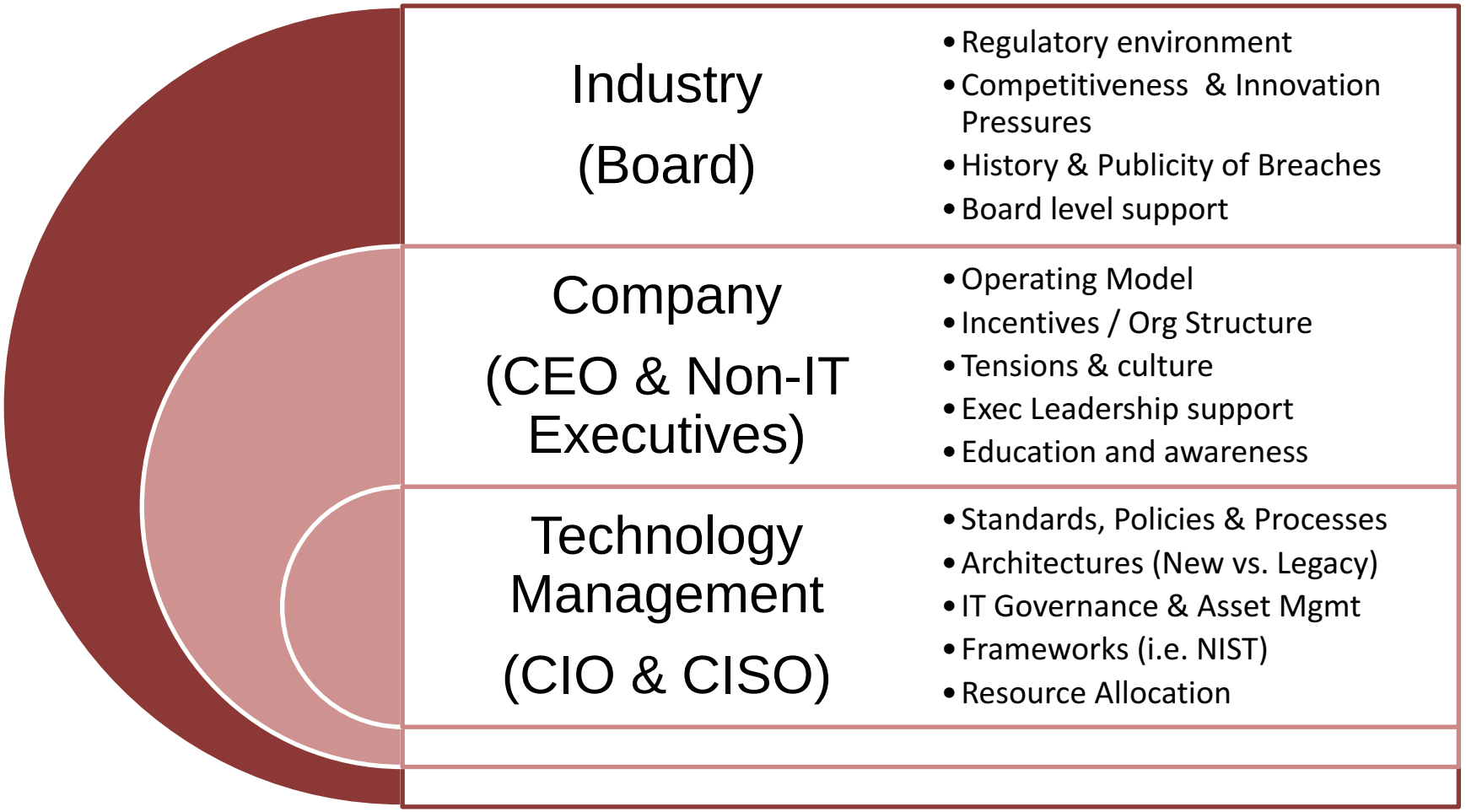


Secure and innovative firms with low negative impact – how do they do it? (7 of 54, 13%)



Size of the bubble - % of Projects negatively impacted by cyber-security control process

Other Factors



Conclusions

- Only 13% of companies are innovating fast and securely, with low negative impact on time to market and scope of innovations

- Balance between innovation, cyber-security priorities and resulting impact is based on a variety of factors in the three categories:
  - Industry environment
  - Company factors
  - Technology management practices

- Even with interested and involved board, “blind spots” in cyber-risk creation may still exist in the middle management of the company

Recommendations

- ❑ Evaluate which quadrant the company is in, and compare with risk & innovativeness profile in other parts of the company
- ❑ Adjust for the industry factors
- ❑ Evaluate board and senior leadership support
- ❑ Examine cyber-risk measurement practices
- ❑ Check for possible misaligned incentives in the org. structure
- ❑ Check for education and awareness at all levels
- ❑ Address current tensions and cultural “blocks”
- ❑ Ensure strong technology management and governance practices, including framework applications
- ❑ **=> If you would like to learn more or get involved with further research, please contact us.**

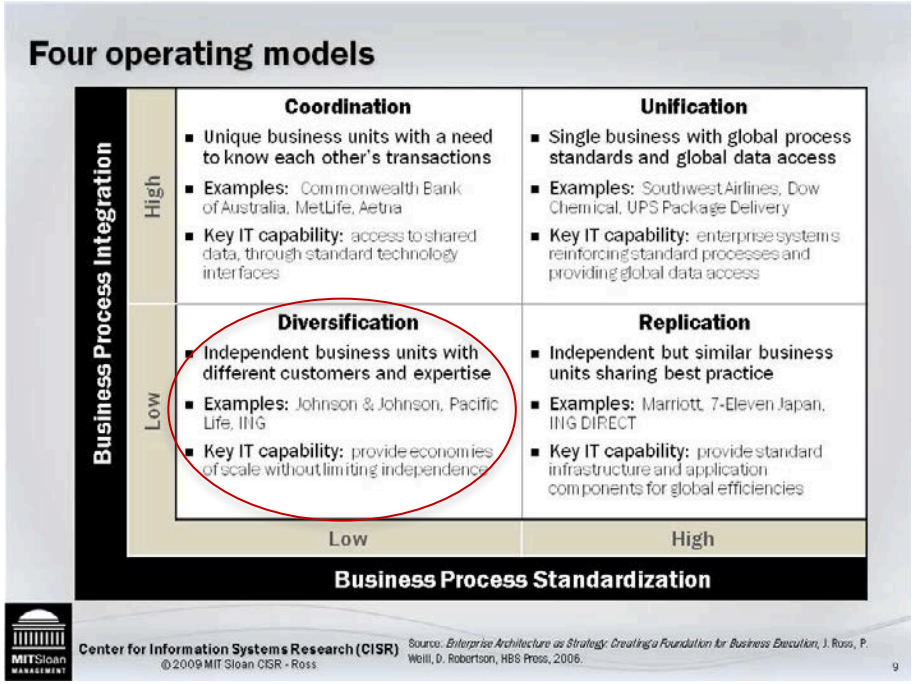
APPENDIX

Industry Impacts

Regulatory	Strong regulations provide good platform for security, serve as a strong driver for executive support, resources and accountability
	Regulated firms need to take a broader view of cyber-security – beyond compliance
	Once established, enables efficient secure innovations
Competitiveness / Innovation Pressures	Strategic product-based, internal or tactical innovations have different characteristics
	Product specific cyber-security approaches: acquisition of specialized cyber-security firm or internal separate cyber-security division not related to IT
	Tactical innovations at operating unit / BU level - hardest to manage
Breach history & Related publicity	Varied by industry, type and purpose / actors
	Publicity of breaches at one company often doesn't translate into applicability to other companies at middle management
	Executives are often most impacted by breaches where executives at other firms were impacted

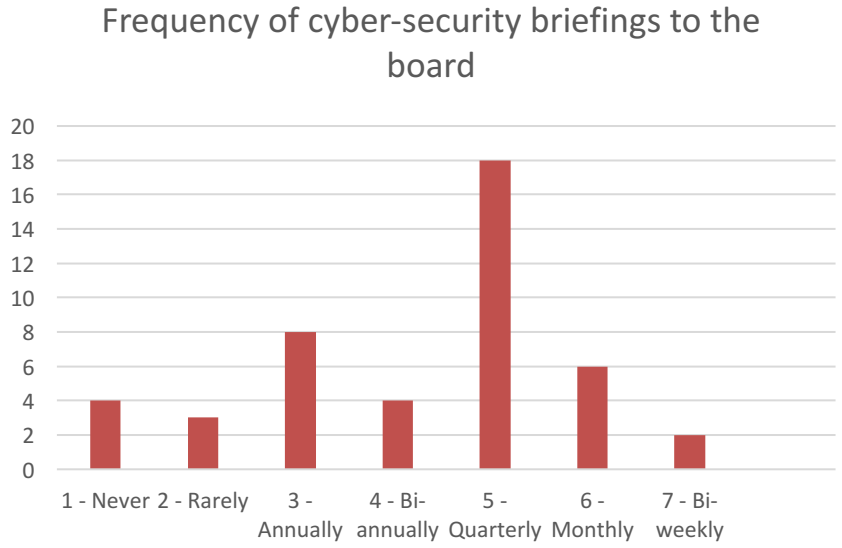
Company Impacts

- Operating Model
  - Impacts innovation and cyber-security efforts in a similar fashion
  - Diversification – hardest on both
- Incentives
  - Ownership / ultimate responsibility for security of the new products
  - Incentives mis-alignment: product focus is associated with tougher awareness efforts
- Tensions & culture
  - Customer Focus and historical safety or security mindset associated with easier awareness efforts



Company Impacts

- Executive leadership support for cyber-security & innovation
  - Strong board level interest in recent years
  - Interactive, quarterly 30-60 minute meetings are most common
  - Many boards are demanding cyber-risk measurement and accountability
  - Technology Innovation briefings and cyber-risk briefings are conducted together (by a CIO and CISO)
  - Board support is critical but not sufficient
- Org Structure
  - Legal teams are starting to play increasingly significant role in cyber-risk analysis & trade-offs discussion
- Education and awareness
  - Board education
  - Managers responsible for innovation
  - Developers



9. Cyber-security Reporting structurePlease identify who cyber-security unit reports to within your...

#	Answer		Response	%
1	Board of Directors		8	13%
2	CEO		9	15%
3	CFO		3	5%
4	CIO		30	49%
5	Legal		2	3%
6	Other		9	15%
	Total		61	100%

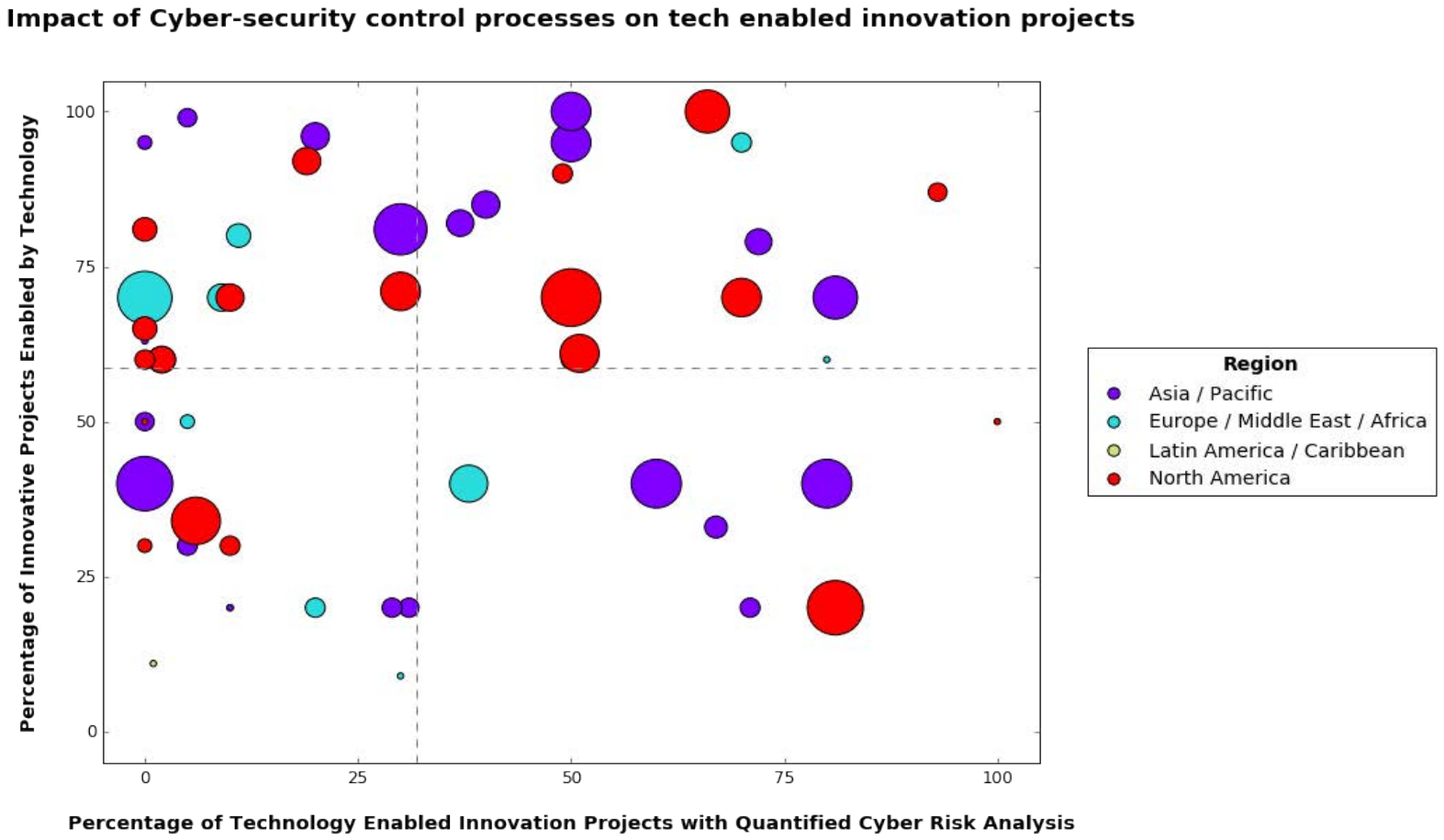
Technology Management

Technology Management Practice	Innovation impact	Security Impact
Standards, Policies & Processes	✓	✓
Architectures (New vs. Legacy)	✓	✓
IT Governance & Asset Management	✓	✓
Cyber-Security Frameworks (i.e. NIST)		✓
Resource Allocation	✓	✓

Business implemented a mobile payment checking with security too late in life cycle causing significant rework of the architecture and implementation of solution with some loss of functionality. However the project did not go live with the risk in place

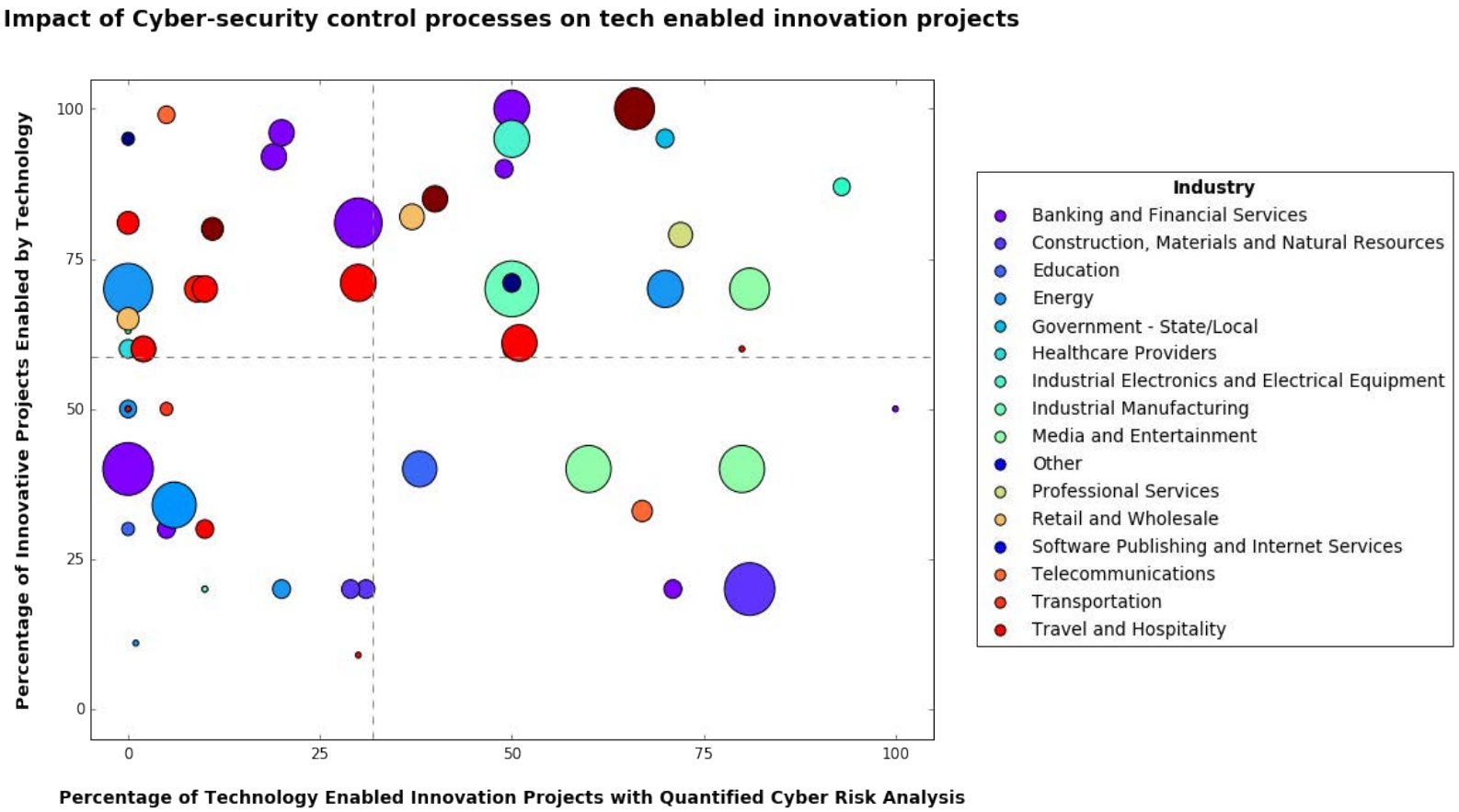
Our SDLC processes do not always include security requirements, due to a lack of awareness and consistent process in development practices. Certain practices and functionalities were enabled knowing that there would be a security exposure. What drove the delivery despite security risks is the desire to provide the functionality to customers, the cost of the project and the timeline to meet commitments made by other business units.

Analysis by Region



Size of the bubble - % of Projects negatively impacted by cyber-security control process

Analysis by Industry



Size of the bubble - % of Projects negatively impacted by cyber-security control process