How companies achieve balance between technology enabled innovation and cyber-security

Natasha Nelson

Working Paper CISL# 2016-01

May 2016

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

How companies achieve balance between technology enabled innovation and cyber-security

By

Natalia (Natasha) Nelson

M.S. Economics
Plekhanov Russian University of Economics, 1993

SUBMITTED TO THE MIT SLOAN SCHOOL OF MANAGEMENT IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF BUSINESS ADMINISTRATION
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2016

Signature of Author:

_____

MIT Sloan School of Management
May 6, 2016

Certified by:

_____

Stuart Madnick
John Norris Maguire Professor of Information Technologies
MIT Sloan School of Management
Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Accepted by:

_____

Stephen Sacca
Director, MIT Sloan Fellows Program in Innovation and Global Leadership
MIT Sloan School of Management

(This page left intentionally blank)

How companies achieve balance between technology enabled innovation and cyber-security

By

Natasha Nelson

Submitted to MIT Sloan School of Management
on May 6, 2016 in Partial fulfillment of the
requirements for the Degree of Master of Business Administration.

ABSTRACT

With increasing economic pressures and exponential growth in technological innovations, companies are increasingly relying on digital technologies to fulfill their innovation and value creation agendas. At the same time, based on the increasing levels of cyber-security breaches, it is clear that the trustworthiness of many established and new technologies is not yet well addressed or appreciated as a fundamental core value in the new digital economy. Consequently, companies are aggressively pursuing strategies to increase cyber-security of their existing and new digital assets. Many CIOs are faced with having to deal with both of these priorities simultaneously and find them to be frequently conflicting, and creating tensions. This exploratory study first introduces a framework for evaluating these risk/reward trade-offs. Through a survey and a series of interviews, companies are positioned in different quadrants on a digital innovation and cyber-security maturity matrix. This positioning is then overlaid with the perceptual negative impact of cyber-security controls on the innovative projects. The thesis then analyzes the industry level, firm level, technology management and the technology maturity factors that affect this perception and these trade-offs. Ultimately the thesis provides a set of practical recommendations for any company to evaluate their own positioning on the innovation / cyber-security matrix, understand the underlying factors that affect that position and how to better manage these trade-offs.

Thesis Supervisor: Stuart Madnick
Title: John Norris Maguire Professor of Information Technologies
MIT Sloan School of Management
Professor of Engineering Systems, MIT School of Engineering

(This page left intentionally blank)

Acknowledgements

First and foremost, I would like to thank my family: my husband Geoff and my sister Olga for inspiring me to go after my dreams, and supporting me in our move to Boston to attend the MIT Sloan Fellows program; my sons, Nicholas and Alexander, for taking on additional responsibilities and independently doing well in school, while I was not around to support them during this year.

Second, I would like to thank my thesis advisor, Professor Madnick, for encouraging me to pursue this theme and allowing me to work with the members of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity to make it interesting and relevant to both the academic as well as the business communities. Also, to Michael Siegel and other members of the consortium for their candid feedback and for providing me with some of the most practical and valuable advice on how to best approach this research.

To David Middelbeck for helping me visualize my framework in the unique and simple to understand manner with the help of the Python data analytics solution.

To my academic advisor Stephen Sacca, for helping me believe in myself and encouraging me to proceed with this work.

Finally, to to the Sloan Fellows Class of 2016 for their support, encouragement, friendships and for helping me unearth the needed data to support this research.

(This page left intentionally blank)

Table of Contents

(This page left intentionally blank)

Chapter 1: Introduction and background

Throughout my career, I have been a part of the evolution of technologists, from "keeping the lights on", to professionals making technology projects successful, to business partners contributing to strategic planning and business transformation efforts. In the last few decades, companies, industries and economies have all experienced a tremendous amount of growth stemming from the various ICT (Information and Communication Technologies) innovations, and I have had the opportunity to be an active contributor to this growth.

How technologies evolved – example from hospitality

At first, technologies were applied to streamline various time-consuming tasks such as accounting work, and then quickly grew in nature and scope. Technology-enabled innovations started to be applicable to streamlining processes that not only saved time, but improved the quality, leading to fewer errors, and ultimately lowering costs. Once process improvements became applicable to various sales and marketing activities, it quickly became apparent that value creation with the help of technologies can not only reduce costs, but also help increase revenues. As an example, in the hotel industry where I worked, the mid to late 90s saw the start of the hotel Yield and Revenue management practices that used historical data and external data sources to forecast the future, optimizing pricing strategies and improving the top line performance. Customer data management and real-time global guestroom inventory distribution transformed the industry, driving sales and providing clear competitive advantage to companies with higher levels of technology sophistication. Many hotel brands implemented loyalty programs, driving more and more guests to their properties.

Following such successes in marketing activities, the sales force and human resources followed the lead, greatly improved their respective performances and expanded their capabilities as their tools became more and more advanced. With the introduction of advanced analytics, companies gained much deeper understanding of the various drivers of their business, extending the preferred decision making techniques to front line employees, managers and automated processes. Additionally, performance management tools became commonplace, allowing CEOs to drive their organizations in the same direction and see the overall picture of what drove their business forward. Communication platforms supporting e-mail, chat, collaborative workspace, idea sharing, on-demand voice and video communications all became possible as global and private networking capabilities matured in speed, cost and availability.

The hotel business also benefited from customer-facing innovations. In hotels, in-room and meeting space technologies have seen a dramatic rise, starting with wired and then

wireless internet access for the guests, Internet Protocol (IP) based High Definition TV and IP Video on Demand, IP Telephony, digital in-room control systems, building management systems, smart door locks and many other significant improvements.

When search and social media became mainstream, hotels' websites and digital content distribution became the next field of competition: TripAdvisor has transformed the way people search for hotels, and various price comparison engines (Kayak, Expedia, Google and others) have forced hotel companies to further step up their game in terms of electronic pricing and distribution capabilities.

Mobile Web, Mobile Apps and IoT are the latest frontier where hoteliers are competing for customers' attention and employees' loyalty. Many physical objects in the "front of the house" (lobby, meeting rooms), in the guestrooms and in the "back of the house" (buildings, elevators, audio-visual systems, door locks, etc.) now come equipped with chips to help manage the hotel and connect with its guests. These various systems connect with each other, privately to the corporate office, to the cloud and to guests' devices via a variety of wired and wireless networks (Wi-Fi, LTE, ZigBee, Bluetooth, RFID and others). Mobile check-in, mobile guest services and mobile phones as door keys are among some of the latest features being offered by hotel companies.

Hospitality is just one of many industry examples where technologies are being used across all segments of the business to improve internal processes and to build revenues with the customers through a growing multitude of external channels. These and countless other examples from other industries demonstrate the enormous value that businesses derive from the latest technology-enabled innovations.

Over the last few years, as technology-enabled innovations grew in numbers, complexity and inter-connectedness, they also became harder to manage, patch and update. Some of these interconnected technologies have come from different vendors, or different internal teams within the same company. Additionally these technologies increasingly have had to interface to or integrate with technologies from other companies. This has led to independent heterogeneous architectures that have necessitated more standardized and integrated operating approaches, development of more industry standards and creation of other mechanisms that would enable the management of these growing unwieldy environments. Data contained in these systems also has grown. It has become more and more difficult to maintain one "master" record for fundamental things such as customer, employee, rate plan, vendor and many other core data elements. These data are frequently spread across multiple systems, located in different networks and different countries, crossing borders and often being left to interpretation.

Many businesses, including hotels, retailers, pharmacies, restaurants and others, are based on the franchised business model. This means that in many cases data is stored on premise at the franchisee-managed location and sometimes replicated in a central facility. This largely depends on the systems architecture, type of data and the need to have centrally managed capacity.

To maintain costs and reduce management complexity, it became customary to outsource various technologies, processes or data management tasks to third parties. Some examples of this include:

- Data center management;
- Database management;
- Software development services;
- IT helpdesk services;
- Call centre management;
- Payroll services;
- HR services;
- Legal services;
- Accounting services.

Finally, the physical infrastructure of hotels themselves became infinitely more complex. Structured cabling, wireless antennas, electronic door locking systems, CCTV cameras, electronic minibars, IP phones, IP Televisions, audio-visual equipment, building management systems, technology "closets" and computer rooms all have grown in complexity and require a growing number of physical and virtual security protection and practices.

The art and the science of IT Management

With the growing complexity of technologies came "the art and the science" of IT management. Quickly growing sophistication of IT management has led to the creation of IT governance frameworks, including physical infrastructure, application management, project management, software development, enterprise architecture, vendor management, services management and others. It has also led to a strong body of research both in the academic and the commercial sectors, a wide variety of educational programs, a sophisticated network of IT supply chains, growth in the importance of the role of CIOs on leadership teams, strong interest in IT-enabled innovations from CEOs and boards of directors, and many other trends. With the explosive growth of tech firms (Amazon, Google, Facebook and others), the competition for top talent became fierce, leaving many non-tech firm CIOs with an even greater challenge of finding the talent required to manage ever-increasing technology transformation agendas. Following the economic downturn of 2008, IT budget allocation and

prioritization processes became further refined and incorporated into the annual budget cycles, as a means to control costs and manage change within organizations.

Increasing complexity as well as concerns for privacy and safety have led to the creation of a wide range of technology regulations and standards bodies, many of which are industry-specific. Some examples include HIPPA (Health Insurance Portability and Accountability Act) for the health care industry, PCI (Payment Card Industry) for any merchant accepting credit card as a form of payment, and many other regulations.

The new cyber-threats

Unfortunately, countries, companies and consumers are not the only parties benefitting from the technological advances. A growing community of hackers and criminals is also taking advantage of the same technological advances, and is innovating at a rapid pace. In fact, the World Economic Forum, in collaboration with McKinsey, conducted a 2014 study that suggests that "if the pace and intensity of attacks increase and are not met with improved defenses, a backlash against digitization could occur, with large negative economic implications". They estimate that "over the next five to seven years $9 trillion to $21 trillion of economic value creation, worldwide, depends on the robustness of the cybersecurity environment". According to the same research, "60% of executives think the sophistication or pace of attacks will increase somewhat more quickly than the ability of institutions to defend themselves. 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 cyber-risk profile."

According to the recent study conducted by KPMG (KMPG International, Cyber security: a failure of imagination by CEOs , 2015), almost one third of the CEOs noted cyber security as the issue that has the biggest impact on their business today. This is a major shift from just a decade ago, where cyber security was perceived to be a tactical problem. The same study asserts that "innovation almost always runs ahead of security. And the bad actors are innovating as well. One of the most innovative marketplaces in the world is the dark net, which supports organized crime as well as basement hackers. Every day there are new tools, new attack services and new cash-out strategies being developed and shared. Everything is changing: the compromise points, the risks and the consequences."

Thesis outline

As a professional CIO, I have experienced first-hand the constant dilemma of the "balancing act" in allocating financial and human resources between the innovation and cyber-security priorities, and managing internal organizational tensions that have arisen from the

conflicting concerns. This thesis sets out to examine different approaches that companies take in making these trade-offs through the use of a three dimensional framework that is meant to track a company's trade-off posture with respect to digital innovation, cyber-security maturity and the perceived negative impact on that innovation agenda as a result of having to address the cyber-security requirements.

The thesis starts out by identifying the value created by technology-enabled innovation, the CIO's role in this value creation, how cyber-security affects this value and in turn, how addressing cyber-security becomes part of this value proposition. An innovation - cyber-security matrix is introduced as a method for evaluating these risk/reward trade-offs, including the perceived negative impact of cyber-security on time to market and scope of innovation projects and where various types of companies would fit in this framework. A survey of 54 companies of different sizes, industries and geographic regions were surveyed with a series of follow-up interviews to test this hypothesis. The companies were placed inside this framework and the results analyzed from the perspective of how cyber risk is measured by the companies and the impact of cyber security control processes on innovation itself. Company industries, regions in which companies were located, and whether cyber security is even measured by these companies were also analyzed in order to identify any trends.

Any analysis of the interviews was used to propose a set of underlying factors that may affect the position of a company in this risk-reward matrix, at the industry, firm, technology management and technology maturity levels. Industry level issues examined include regulatory compliance requirements, competitive innovation pressures and cyber breach publicity. Organizational factors included the business operating model, company culture, impact of the board of directors and internal education regarding cyber security. Technology management practices reviewed were the impact of IT standardization, legacy architecture, IT governance and resource allocation. Three current trends in innovative technologies, payment processing, IoT (Internet of Things) and Blockchain, are then used as a proxy for varying degrees of technology maturity to determine how that factor may affect value creation for the business and be affected by potential or actual cyber risks.

Ultimately the thesis provides a set of practical recommendations for any company to evaluate their own positioning on the innovation / cyber-security matrix, understand the underlying factors that affect that position and how to better manage these trade-offs.

Chapter 2: Technology-enabled innovation

Value created by technology-enabled innovations or digitization

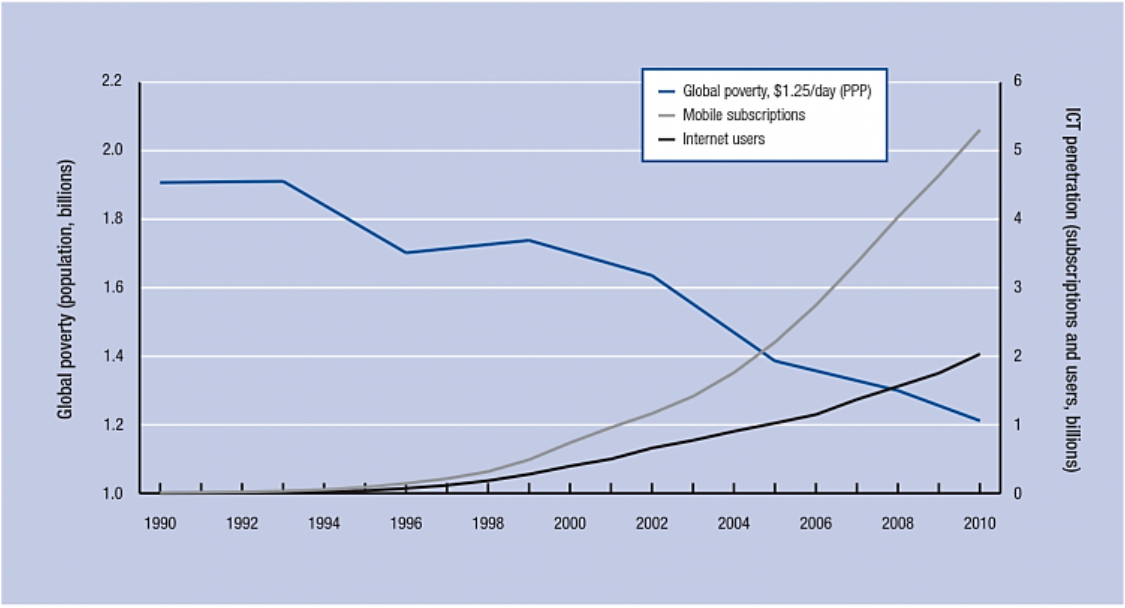
From the macro-economic stand point, ICT innovations have had direct as well as indirect effects on the GDP growth. According to the research conducted for the World Economic Forum, there are four main mechanisms responsible for the GDP contributions from the ICT sector. They are:

- Impact driver #1 (direct) – "ICTs contribute to GDP directly through the production of ICT goods and services as well as well through continuous advances in ICT-producing sectors";
- Impact driver #2 (indirect) – "ICTs contribute to total factor productivity growth through the reorganization of the ways goods and services are created and distributed";
- Impact driver #3 (indirect) – "ICT industries generate positive employment effects";
- Impact driver #4 (indirect) – "increasing applications of ICTs (capital deepening) leads to rising labor productivity" (Pepper and Garrity, 2016).

To clearly demonstrate the concrete economic impact of ICT innovations, the WEF and the World Bank have tracked the trends in the global extreme poverty rates (defined as those individuals who survive on less than $1.25 per day), which has dropped from 1.9 billion people in 1981 to 1.3 billion in 2010. This drop, according to the World Bank, was driven by the economic growth in China, India and Africa, and the impact of social programs in Latin America. Although the causality is not established, we can see that as poverty has declined, more and more people in those countries have gained access to the internet and mobile phone subscriptions. **Figure 1** demonstrates this phenomenon.

Figure 1 - Falling global absolute poverty and rising ICT penetration

Figure 1: Falling global absolute poverty and rising ICT penetration

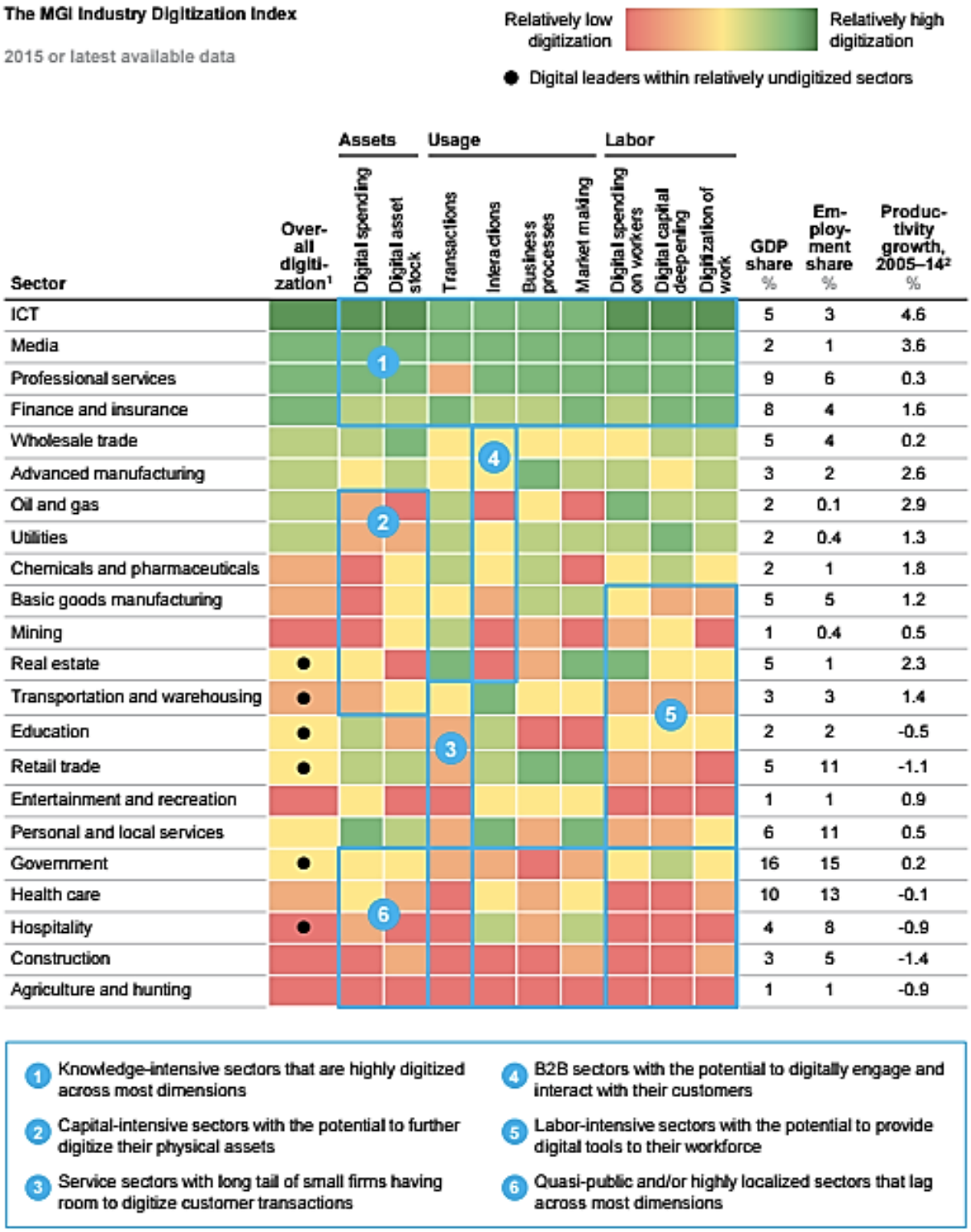


Sources: World Bank *PovCal* database (1990, 1993, 1996, 1999, 2002, 2005, 2008, 2010); authors' calculations and interpolation, ITU *World Telecommunication/ICT Indicators* database June 2013.

In the rest of the document, I will refer to these ICT innovations as "technology-enabled" and where possible, focus on the value creation aspect of it.

Within the private sector, value creation and corresponding value extraction from technology-enabled innovations came primarily from the impact drivers #2, #3 and #4. Specifically, growth came from a variety of technology-enabled, value creating innovations that have been adopted by companies, industries and consumers. Recently, the McKinsey Global Institute has introduced the MGI Industry Digitization index, demonstrating the advantage in profitability achieved by those industries and companies that are operating on the "digital frontier".

Table 1 – MGI Industry Digitization Index



This research asserts that the gaps between more and less digitized industries underscores not only the challenge of continuously adapting but also the size of the opportunity still ahead. In fact, some of the sectors that are currently lagging could be poised for rapid productivity growth. Companies in manufacturing, energy, and other heavy industries are investing in digitizing their extensive physical assets, bringing us closer to the era of connected cars, smart buildings, and intelligent oil fields (McKinsey. *Digital America: A tale of the haves and have-mores*. McKinsey & Company, 2016, page 4).

CIOs role to direct the technology-enabled value creation agenda

The velocity of the technological innovations that are being adopted by companies is constantly increasing. According to the Accenture Technology Vision 2015, "62 percent of business and technology executives are investing in digital technologies, and 35 percent are comprehensively investing in digital innovation as part of their overall business strategy" (page 6).

At the 2016 WEF event (Schwab, Klaus. *World economic forum annual meeting 2016*), Meg Whitman, the CEO of Hewlett Packard, focused specifically on the increasing speed of technology-enabled innovation:

> My view is that the future belongs to the fast. If you can't get your organization to accelerate at dramatic speed, their ability to develop the technology that would allow you to win, almost by definition, you are falling behind. The other thing is that business strategy is now completely one and the same with IT strategy. And almost every company has an existing, quite rigid, not cost effective, slow legacy IT environment that's been built up from anywhere from 10 to 50 years. And every organization knows that they need to move from where they are to where they must be. And so, how do you balance the needs of your existing IT infrastructure that runs your business, runs your supply chain, while at the same time you move to the new environment?

In this increasingly fast, complex and competitive environment CIOs are required to play an increasingly strategic role in the organization and are called upon to deliver new innovations empowered by technology. According to the joint IDC and Forrester predictions (Golden, Bernard. *5 IT industry predictions for 2016 from Forrester and IDC*. CIO, 2015), for 2016 in the CIO Magazine, enterprise IT is entering another 5-year cycle where many technologies will be redefined and new vendors will take center stage. Specifically, the following 5 trends for 2016 are being projected:

1. "Legacy vendors face a bleak future";
2. "Cloud providers will be winnowed down";
3. "Big data gets, well, big";
4. "Enterprises turn into software companies";
5. "Developers are the scarce commodity".

According to the same forecast, "corporate IT is about to see its role and expectations change as never before. For many, this will be disconcerting. As I often put it: For years, IT has asked for 'a seat at the table.' It's terrifying when you finally get a seat and then everyone turns to you and asks 'what should we do?' ".To support this trend, according to MIT CISR Research (Table 2 below), the percentage of time that CIOs spend on the innovation agenda has strong positive correlation to the overall company's performance, and the difference between top performances and bottom performances is significant.

Table 2 – Percentage of CIO time spent on innovation

	Bottom 25% Margin Companies, relative to Industry average	Top 25% Margin Companies, relative to industry average
Percentage of CIO time spent on innovation	19%	53%

Source: MIT CISR 2015 Digital Disruption Survey, N=414.

As we can see from this table, CIOs that work in the 25% of companies achieving the lowest profit margin relative to the industry average spend 19% of their time on innovations, while their peers at the companies in the top 25%, spend 53% of their time on innovation. This difference has strong statistical significance and demonstrates the significance of innovation agendas for CIOs relative to company performance.

Negative impact of cyber-security related losses

On the other hand, many CIOs continue to maintain the responsibility for the on-going management of the cyber-security efforts; they are constantly increasing investments in cyber-security technologies, processes, projects, talent and education. The last few years have seen a tremendous increase in the number as well as the pay scale of the Chief Information

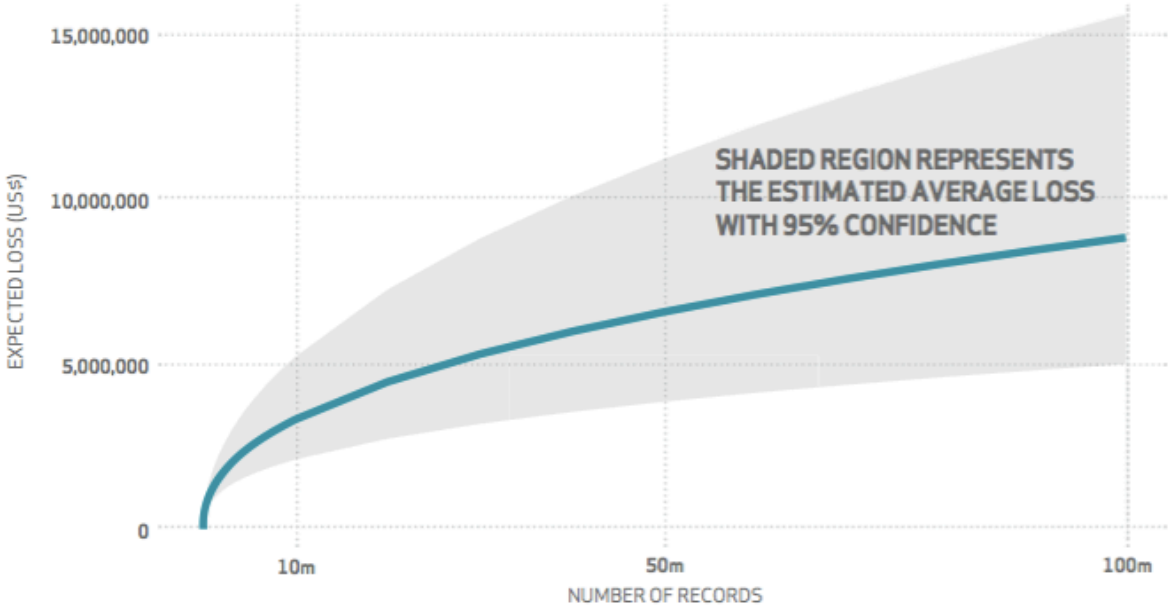
Security Officers (CISOs), who usually report to CIOs, and are required to regularly attend the board of directors meetings with a cyber-security briefing.

Much like the positive impact of the technology-enabled innovations, the negative impact of cybersecurity related losses can also be split into direct and indirect components.

Direct negative impact of cyber-security related losses

The direct impact comes from "successful" breaches achieved by hackers. This impact is easier to quantify: according to the Verizon's 2015 Data Breach Investigation report, 70 surveyed companies recorded 79,790 security incidents and 2,122 confirmed data breaches (page 1). According to the same report, the cost of a breach of 1,000 records ranges between $52,000 and $87,000. Figure 2 below demonstrates these calculations.

Figure 2 - Expected average loss by records lost

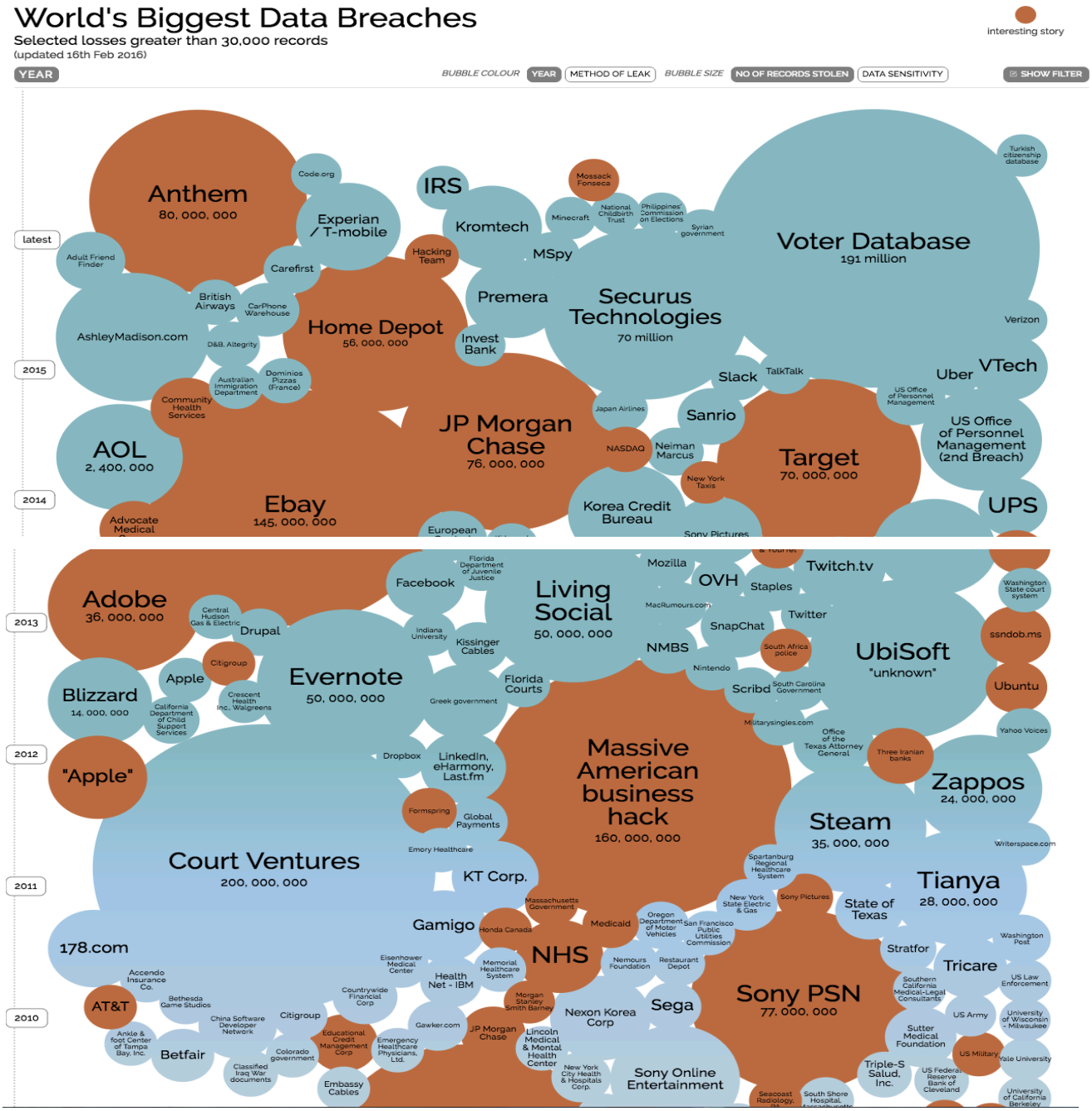


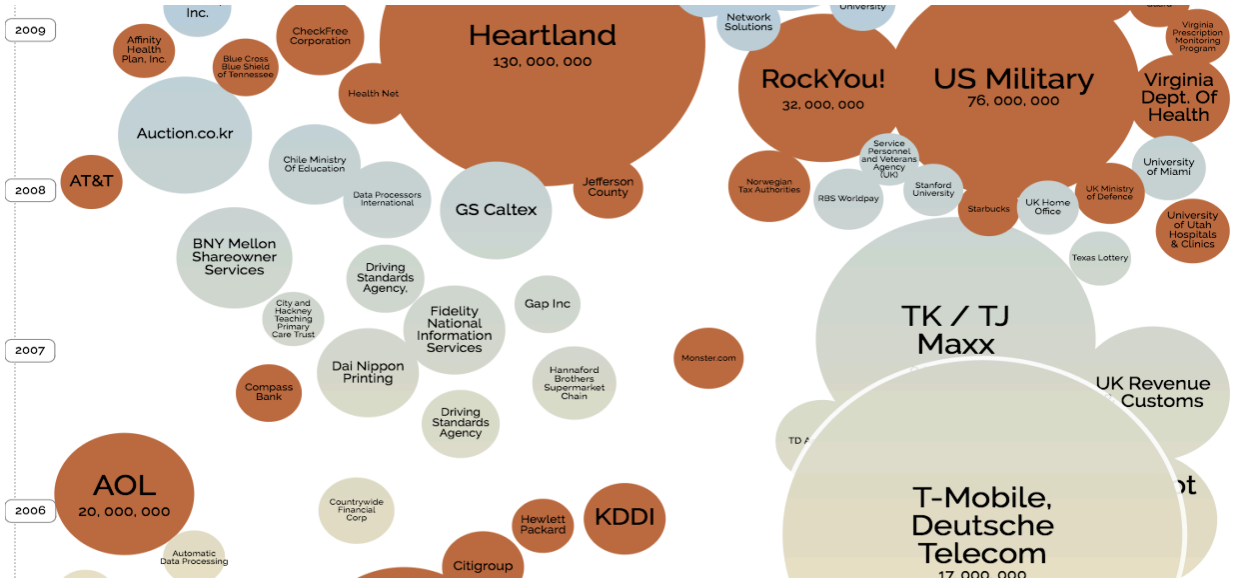
36 Look for more details behind this model in the coming year.

2015 DATA BREACH INVESTIGATIONS REPORT

To further explore the number of breaches, their size and frequency, the "Information is Beautiful" website has put together the following infographic.

Figure 3 – World's Biggest Data Breaches





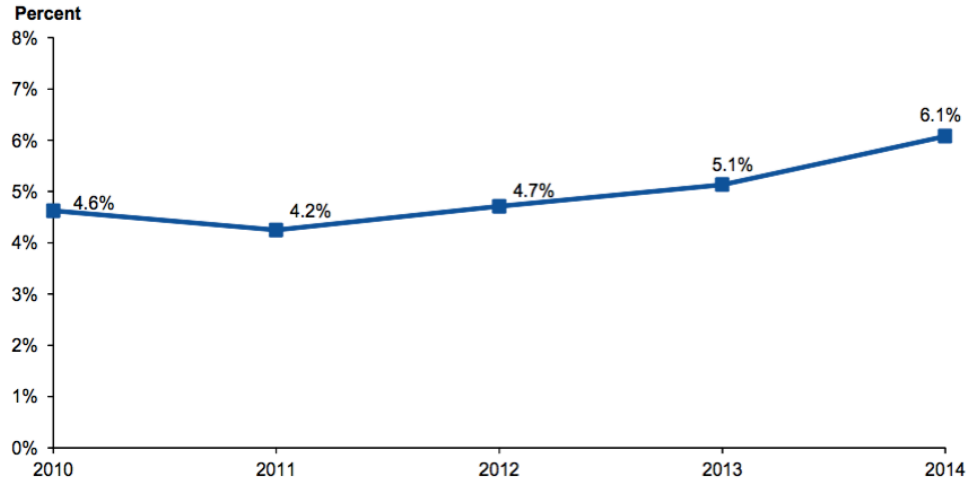
Source – Information is Beautiful

As we can see from this infographic, both the size and the breadth of cyber breaches have been increasing over the last few years. From a well-publicized TJ Maxx attack in 2007 to the Sony attack in 2010, with the most recent being JP Morgan Chase, Target, Home Depot, Anthem and the Voter Database, these attacks are likely to continue and grow in size. The hacks into Ashley Madison and Mossack Fonseca also suggest new levels of sophistication and different motives for the attackers.

Indirect negative impact of cyber-security related losses

The indirect source of value loss is much harder to quantify: it comes from displaced resources, increased caution (warranted or unwarranted) of moving forward with the new technology-enabled innovations and inefficiencies caused by the necessary cyber-security reviews (delays and scope reductions). The resource implications can be quite clearly seen from the Gartners' IT Key Metrics Data 2015 report on Key IT Security Measures: Multiyear. IT Security spending as a percent of the overall IT spending has been steadily increasing, and therefore decreasing the other parts of the IT Spending "pie" (page 9) – please see Figure 4 below. This increase in IT Security spending effectively displaces the investments in other areas of IT, and could be particularly challenging to justify in terms of Return on Investment.

Figure 4 – Total IT Security Spending as a Percent of IT Spending, 2010 – 2014

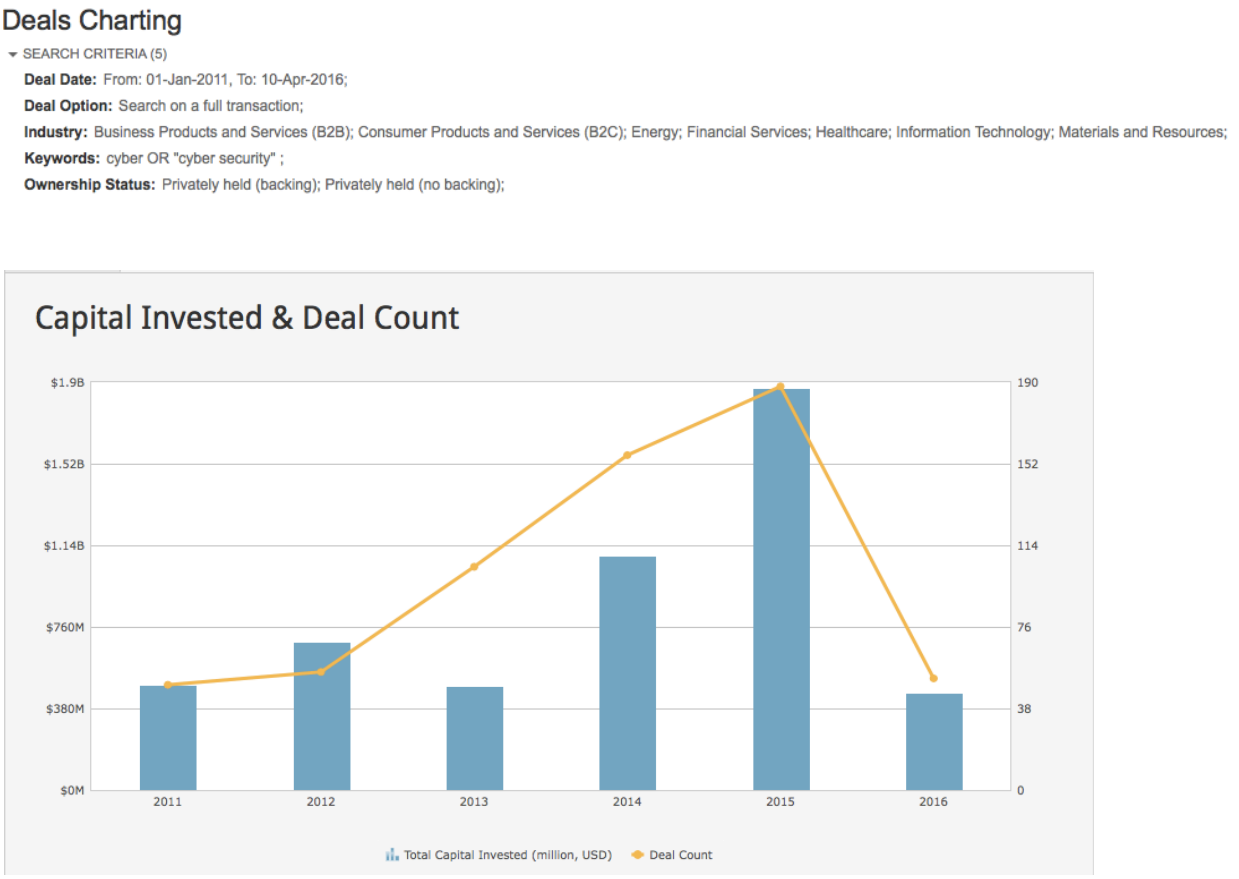


Source: Gartner IT Key Metrics Data (December 2014)

The implications of increased caution and inefficiencies can in part be traced to the complexity of identifying the appropriate cyber security solutions for the business. Two ways of measuring this complexity are the growth of the IT Security market as show through Venture Capital investment in cyber security firms and the fragmentation of the cyber security industry itself.

The first indicator of this complexity is the growth of the size of the IT Security market, and more specifically, Venture Capital investments in companies that are selling IT Security products. We can examine privately held and VC-backed cyber-security related activities over the last five years, as the market would anticipate the future value over the next 5-10 year timeframe. Venture Capitalist activity continues to grow, although in the recent months the activity has been cooling off, due in part to the fragmented market and the apparent lack of quickly growing cyber-security firms. **Figure 5** below represents the trends of the invested capital in the cyber-security space and further supports the growing interest in this field and the growing expectations. The drop in 2016 is consistent with reporting only partial year figures.

Figure 5 – Capital Invested and Deal Count: Cyber-security



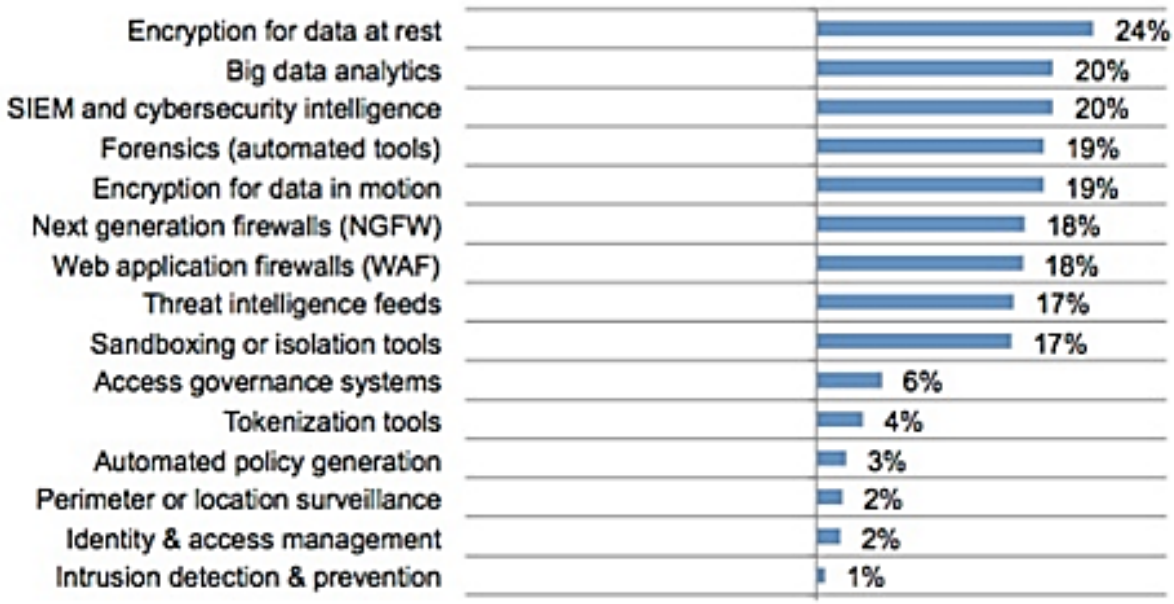
Source – PitchBook

The second indicator is the fragmentation of the cyber-security firm market, often described as "crowded". In the TechCrunch article "Cockroaches Versus Unicorns: The Golden Age Of Cybersecurity Startups" (Mahendra Ramsinghani), the author clearly explains the issue that current CISOs are faced with: "CISOs want peace of mind in trusted partnerships. If they have a problem, do they trust you enough to call you in the middle of the night? They prefer to have comprehensive (not niche) solutions, which can be integrated within their existing systems and are built by security experts. While all products claim to be robust and reliable, CISOs need "IBM-like" solutions that can be defended in the boardroom. After all, their jobs are on the line" (Mahendra Ramsinghani). Since the cyber-security market is based on trust, CISOs are looking for a comprehensive approach, one that would cover all of their bases.

These indicators of an overwhelming number of niche products creates a lot of confusion, and CISOs instead would prefer to go to a larger outsourced provider to procure these services. Therefore, many large service companies, such as IBM and large Telcos are positioning cyber-security as one of the key growth areas. Furthermore, to keep track of the various activities, threats, risks and remediation, CISOs are looking more and more towards robust analytics solutions.

While large companies are positioning themselves to be a "one stop shop", it has not yet materialized, and the buying process continues to be complex and fragmented. Consequently, many companies are not able to find and implement those solutions that would maximize their cyber-security capabilities, which in turn may lead to either increased caution and therefore less innovation or breaches and more direct negative impacts. Figure 6 below represents the top trends for the cyber-security products, and speaks to both the complexity and fragmentation of the cyber security market.

Figure 6 - Global Megatrends in Cyber Security



Source: Global Megatrends in Cyber Security, Ponemon Institute, March 2015

Trade-offs

Finally, there are a series of trade-offs that companies make that may potentially lead to either direct or indirect cyber-security related losses. From the academic research stand point, David D. Clark at the MIT C.S.A.I.L. center in his December, 2015 article "The Landscape of Cyber-security" attributes, in part, some of the cyber-security flaws to the motivations of the economic players.

> 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. (Clark, p11).

Examination of these tensions is one of the key points of this research. Several of the following chapters will help examine these tensions both quantitatively and qualitatively.

Cyber-security – fundamental to product value

Given the competing innovation and cyber-security priorities that companies and CIOs must balance, one useful "reconciliation" philosophy is that of an investment in trust that the customers will have in the firms' products. This argument was presented very strongly by Marc R. Benioff, Chairman and Chief Executive Officer, Salesforce, on the same panel at the World Economic Forum 2016. Here is an excerpt from the transcript of his talk:

> The fourth industrial revolution starts with one very important point, which is trust. That is – you are about to define a new level of trust between yourself and your employees, between yourself and your customers, between yourself and your key stakeholders, between yourself and your shareholders, between yourself and your partners.
>
> And, this is a cultural revolution for organizations that are not built on trust, because when we talk about trust, when we talk about growth, when we talk about innovation, we have to talk about it in that order. That's number one.
>
> This morning, I went to the gym and I see the CEO of Technogym in there. He has all this amazing new equipment, and it's all connected now and I have to put in my information. It's a bit Internet of Things, and his bikes are connected, and the elliptical trainers are connected, and the treadmills are connected and he knows who I am, how much I'm working out, he's got all my biometrics, and it's not just about B2C, because he's also a B2B company, that is he is selling to the hotels, to the fitness centres, and he is building this collaborative social network. So, it's about mobility, collaboration, the cloud, because now he has a big Technogym cloud, but at the end of the day, I'm only

going to use those bikes, and I am only going to register on the network and I am only going to get involved if I trust him.

As a customer, I better be ready to accept a new level of trust, because of the types of access, the types of information, the types of data, and the level of privacy that we are talking about. It doesn't matter if you are HP, or Alcoa, or Schneider Electric or Kaiser – all of these companies are going on line. All of these companies are connected in a whole new way, and they are connected to their customers in a whole new way. They all have incredible stories about how this fourth industrial revolution is transforming them, not only now, but where they want to see themselves 10 years from now, but I guarantee you that in each and every one of these stories it begins with the transformation of trust in the enterprise, and that's the hard part. Employees better realize that customers are not going to use your products in the fourth industrial revolution unless they trust you. This is a big change.

The opportunity is to get to the future fast, and then make sure you show up with the right values, because the values in the fourth industrial revolution are different."

From the academic research stand point, David Clark also supports this but goes one step further to define the new actors as "not mutually trusting", and thus new solutions for creating trust in such environments will require new ways of thinking:

"Part of what defines the experience of using the Internet is trying to create a trustworthy experience in a context where we must accept and tolerate actors that are not mutually trusting, and who do not have aligned interests."

To summarize these key points, the new "digital trust requirement" will become increasingly apparent and necessary for future innovations, specifically:

- Digitization requires a new level of trust as a vital ingredient of success;
- Trust is required for all stakeholders – employees, customers, shareholders, partners;
- To achieve this new levels of trust, many companies need to make cultural changes;
- Trust must be established in the context where not all actors are mutually trusting.

In order for trust to be effective, Cyber-security will have to become one of the key investments in this future, because without strong cyber-security capabilities it will be impossible for companies to earn and maintain the trust of their customers, employees and shareholders, particularly for financial transactions. This means cyber-security becomes a fundamental part of the value of the product or service that the customer receives. Trust in cyber security and in data privacy then becomes a core value that must be fundamental to future digital products and services. Ensuring that trust is part of the value proposition of

innovative products and services contributes to the tension between cyber-security and innovation as to be trustworthy, innovative technologies must address cyber-security.

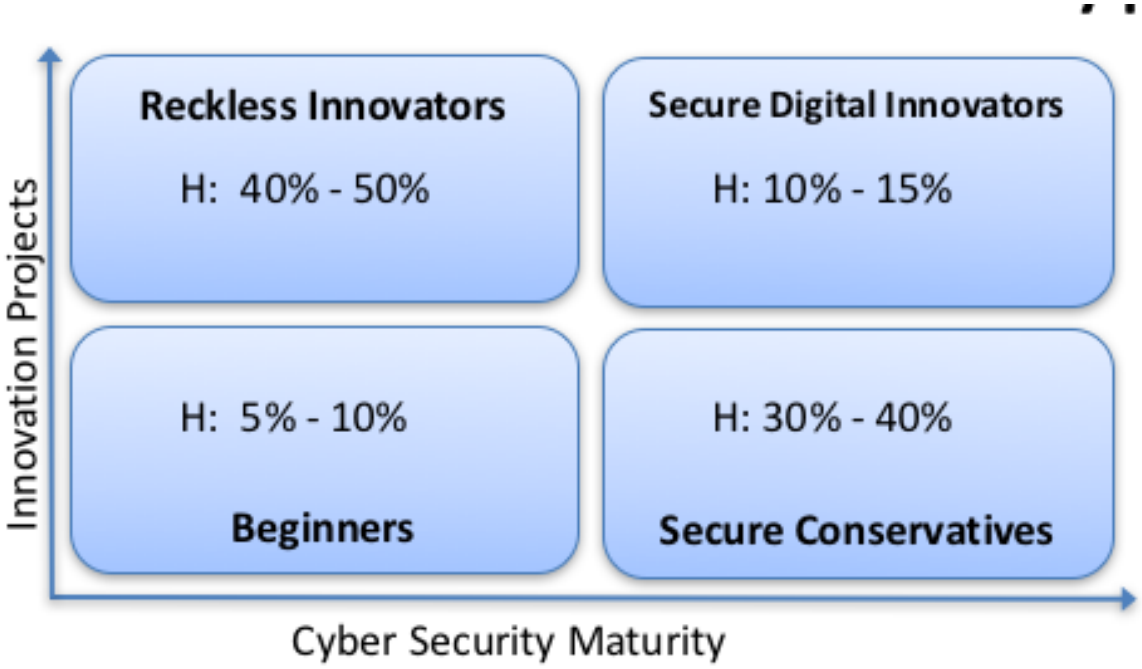
Initial framework and hypothesis

To examine the relationship between different factors and related trade-offs, I started my research project by building a simple framework (see Figure 7) that plots companies into four different quadrants as follows:

- The X axis would measure the maturity of cyber-security within an organization;
- The Y axis would measure to what extent an organization depends on technologies to execute their value creating innovation agenda.

Based on these measurements I proposed to deeper examine which companies would fall into various quadrants, and find underlying factors that would move companies into those quadrants.

Figure 7 – Cyber Security Maturity and Innovation matrix



Based on my own intuition, experience and on-going monitoring of the articles on a variety of related subjects, I hypothesized the following:

- 5% - 10% of the companies would be "below average" on both the "Technology Innovations" as well as "Cyber Security Maturity" measurements; I called this group "The Beginners";
- 30% - 40% of the companies would be "below average" on the "Technology Innovations", but above average on the "Cyber Security Maturity" measurements; I called this group the "Secure Conservatives";

- 40% - 50% of the companies would be "above average" on the "Technology Innovations", but below average on the "Cyber Security Maturity" measurements; I called this group the "Reckless Innovators";
- 10% - 15% of the companies would be "above average" on both the "Technology Innovations" and on the "Cyber Security Maturity" measurements; I called this group the "Secure Digital Innovators".

One of the goals of this thesis is to test these hypotheses and see what percentage of companies surveyed fall into each quadrant, get a deeper understanding of what types of companies are in each quadrant and why. This would allow CIOs and CISOs to compare themselves using this framework, get a better understanding of the reasons of why they are where they are and perhaps find practical approaches to enhance or move into a different position.

Chapter 3: Quantifying the impact of cyber-risk management on innovation

Analysis of survey respondents

To get deeper understanding of the relationship between the technology-enabled innovations and cyber-security concerns, I conducted a survey from December 2015 to January 2016. The survey was distributed via multiple channels:

- My own professional network of managers and executives;
- Select members of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity;
- MIT Sloan Fellows class of 2016 and their professional networks;
- Select MIT Sloan Alumni with specialization in IT and several years of executive experience;
- CIO Association of Canada;
- Hotel Technology Next Generation – which is a trade association with the focus on hospitality industry.

Although, understandably, many survey participants forwarded this survey to their IT and IT Security managers, it was important to also gather opinions of non-IT executives.

Here are some basic facts about the survey:

Table 3 – Survey Responses by region and industry

Row Labels	Asia / Pacific	Europe / Middle East / Africa	Latin America / Caribbean	North America	Grand Total
Banking and Financial Services	6			3	9
Construction, Materials and Natural Resources	1			1	2
Education		1		1	2
Energy	1	2	1	1	5
Government - State/Local		1			1
Healthcare Providers				1	1
Industrial Electronics and Electrical Equipment	2				2

Industrial Manufacturing	1			1	2
Media and Entertainment	2				2
Other		2	1	1	4
Professional Services	2			1	3
Retail and Wholesale	1			1	2
Software Publishing and Internet Services	2			2	4
Telecommunications	2				2
Transportation	1	1			2
Travel and Hospitality		3		8	11
Grand Total	**21**	**10**	**2**	**21**	**54**

Table 4 – Survey Responses by region and the role of respondent

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**

Table 5 – Survey Responses by region and the size of the organization (size determined by number of employees)

Row Labels	Asia / Pacific	Europe / Middle East / Africa	Latin America / Caribbean	North America	Grand Total
Large (10,000 or more)	4	4	1	4	13
Medium (1,000 to 9,999)	14	4		10	28
Small (fewer than 1,000)	3	2	1	7	13
Grand Total	**21**	**10**	**2**	**21**	**54**

When designing the survey questions, I realized that both cyber-security maturity and the level of technological innovations within companies is not a well measured or commonly measured metric. As such, I created questions that served as proxies to these measures. To ensure maximum accuracy, I used two specific survey techniques:

- Questions focused executives' attention on the activities over the last 12 month period, to ensure that the responses are not perceptual, and are fresh in their mind;
- For each question, specific examples were provided to help make questions less abstract and cover the spectrum of what's possible.

I will now review the results on a question by question basis.

Cyber-risk measurement

Who is measuring cyber-risk and why

For the proxy of "cyber security maturity" on the X axis of the framework, I used the notion of cyber-risk measurement: the rationale of using this measure is that when companies are making a choice to accept a certain amount of cyber-risk, perhaps they would understand the nature of this risk. Here are the results of the risk-measurement question.

Table 6 – Measuring cyber-risks

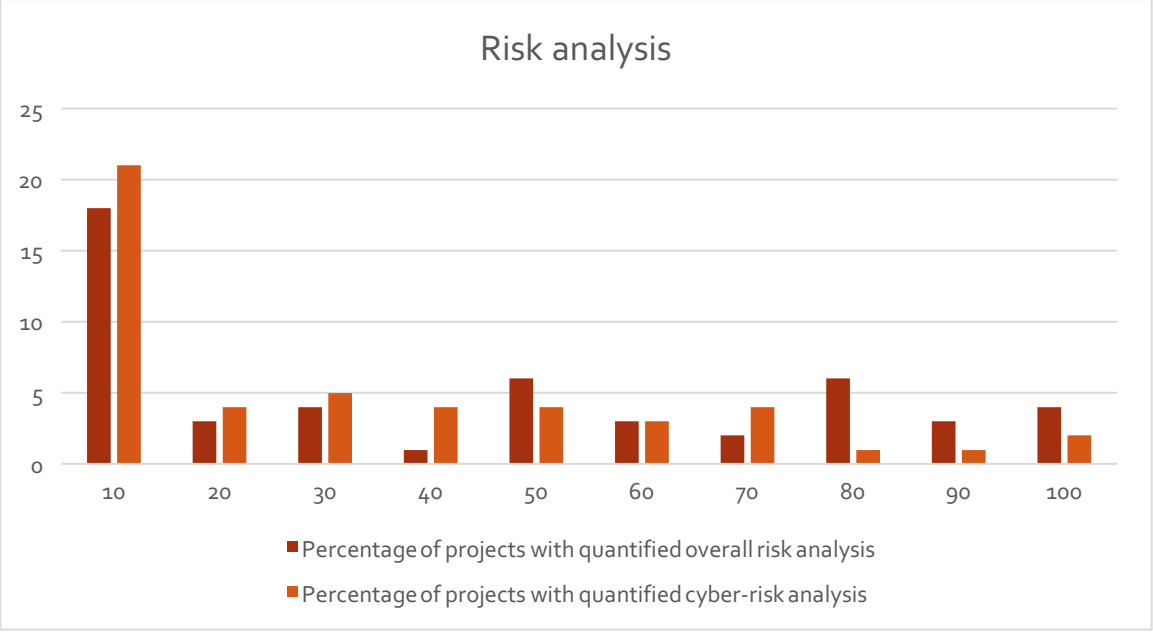
Measuring cyber risks

To the best of your knowledge, in the approval process of these technology-enabled initiatives, what percentage of them included quantified risk analysis, including measured cyber-risk?

Examples of measurable risk analysis
- Estimated percentage of defective parts, and associated replacement costs
- Number of late deliveries and associated costs

#	Answer	Min Value	Max Value	Average Value	Standard Deviation	Responses
1	Percentage of projects with quantified overall risk analysis	0.00	100.00	40.26	33.80	61
2	Percentage of projects with quantified cyber-risk analysis	0.00	100.00	29.69	29.01	59

Figure 8 – Risk analysis



From the data shown in Figure 8, we can see that even overall risk measurement on projects is not a common practice, and cyber-risk measurement in particular trails behind. That being said, an interesting observation can be made about companies that have a strong discipline of measuring the risk of almost all of their projects (>80%): even those firms have not fully embraced cyber-risk measurement into their usual risk measurement practices.

Although some degree of cyber-risk measurement is definitely present, based on the interviews conducted it is clearly not a developed area and needs a lot of attention. Despite imperfections of the measurement methodologies, those that measure their cyber-risk or cyber-security activities achieved a greater degree of transparency and changed behaviors (as will be demonstrated in a later chapter). In some instances, there appears to be "too much" reporting that is simply too complex to understand. These reporting mechanisms are not as effective and don't generate the same positive results.

Here is the list of approaches around cyber-security measurement and reporting:

- The most powerful mechanism discovered was measurement of cyber-security compliance by business unit or department. This was implemented by companies that operate in a decentralized environment, and whose efforts largely depend on the effectiveness of the local teams in their adherence to standards and compliance activities. This approach creates accountability at the business unit level, driving the desired behaviors and providing necessary authority to the cyber-security teams;
- One of the companies that manages a combination of franchised and owned business units created two separate dashboards so that the executive leadership team and the board can track their risk based on the business model;
- Another powerful and effective approach utilized by one of the interviewees operating in a centralized operating model firm tracks their cyber-risk activities using the "layered" approach: assets, data, application, end point, network and perimeter. Within each layer, color coding is used to represent the level of significance, and visual display is used to separate currently employed processes from future planned efforts and projects;
- Another well managed decentralized firm folds cyber-risk reporting into the overall Enterprise Risk Management dashboards, but clearly identifies it as cyber-risk. While risk areas are described, their impact on the enterprise is categorized as high, medium or low.

Perhaps the most critical aspect of all aforementioned reporting mechanisms is their usage: those dashboards that are frequently presented to the board and are actively discussed in the board meetings tend to be better adjusted to be easily understandable and generate right behaviors and incentives within the organization.

Examples of the two opposite cyber-risk measurement practices

To demonstrate the spectrum of the cyber-risk measurement practices, I would like to share two examples from an interview with a CIO from a Pan-European transportation company. This company owns several entities, and as such, their CIO was able to demonstrate both "ends of the spectrum" right from within his firm.

In the first example, a company is very risk adverse, which in large part is due to the historic attention to the life safety requirements. In this case, they think of cyber-risk and life safety at the same time. Here is the process that company follows:

- When a project starts, a single page project description is submitted to a steering committee;
- If the steering committee deems this project to have some potential, they require that a project charter gets created. Among other things, the project charter must include risk and benefit analysis;
- The company has three security professionals: physical security, information security and technical security, and all risk is also being reviewed by the legal team right at the beginning of each project prior to its initiation;
- Based on the project charter, investment decisions are made;
- Since the company culture is very risk adverse, there is a clear rule that "we are not willing to do anything that others haven't done before". This applies even in the cases where with extra effort and some creativity, security risk can be significantly mitigated, but unwillingness to be the first always "rules";
- Finally, the speed of project delivery is quite slow.

By contrast, under the same holding company, there is a small firm operating like a lean start-up, where the only risks that are looked at are legal and financial, and no other risks are ever considered.

Summary of the insights

- Although there is currently no standard in cyber-risk measurement and reporting, a variety of approaches exists and is being used actively, adding transparency and efficiency;
- Measurements that are easily understandable and are actively discussed at the board meetings are most effective;
- Those dashboards that properly align measurements with the organizational structure and risk tolerance drive the right behaviors;
- In some instances, cyber-risk reporting is embedded within the Enterprise Risk reporting toolset.

Technology Enabled Innovations

For the proxy of "technology enabled innovations" on the Y axis of the framework, I focused on the percentage of innovative, value creating projects enabled by technologies. Although it is quite easy to imagine innovations enabled by technologies, many companies in various industries innovate in other ways. For example, in the restaurant business, innovation may come from a chef's new recipe or mix of ingredients, while in the finance industry it may come from a new financial product. Therefore, the percentage of innovative projects that were enabled by technologies helps us understand to what extent a company relies on digital technologies to support their innovation efforts. As this number goes up, technology management practice in a company becomes more strategic, the number of used technologies increases in volume and might create more cyber-risk.

Here are the results of the innovation measurement question.

Table 7 – Technology enabled innovation projects

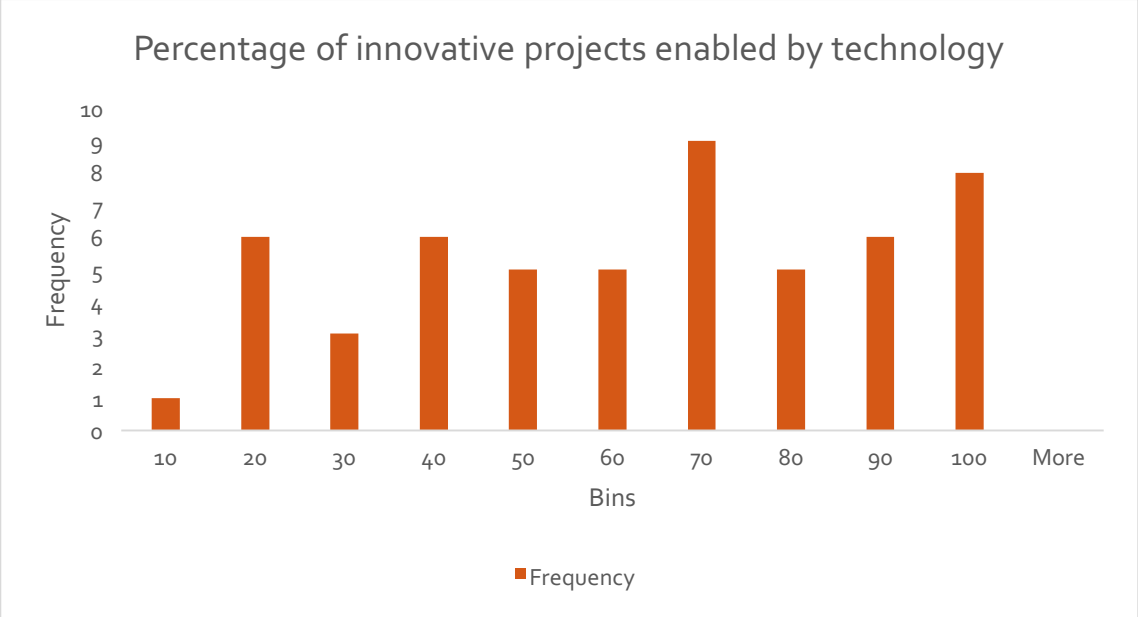
Technology enabled innovation projects

In the last twelve months, to the best of your knowledge, approximately what percentage of value-creating, innovative projects undertaken by your company or organizational unit were empowered by or enabled by technology? Value creation typically comes from projects that generate revenues, save costs, generate efficiencies, improve customer experience or improve product.

Select examples of value creating technology enabled projects
- **Mobile Applications for customers or employees**
- **Cloud Computing Services and Data center cost reduction projects**
- **ERP, Human Capital Management or Supply chain systems**
- **E-commerce or Mobile Commerce**
- **Internet of Things Projects**
- **Big Data or Business Intelligence projects**

#	Answer	Min Value	Max Value	Average Value	Standard Deviation	Responses
1	Percentage of value creating innovative projects enabled or empowered by technology	9.00	100.00	61.89	24.70	71

Figure 9 – Histogram: Percentage of innovative projects enabled by technology



We can see that there is a large spectrum of reliance on technology for enabling firms' innovation agendas, with an average of 62% and a significant number of companies in the 70% and above group. This finding is very much in line with the McKinsey MGI index. This is especially important given the fact that there are very few high tech firms in the survey, so this finding is quite relevant across the broad range of industries.

Interestingly, the 2016 World Economic Forum conference had a theme of the "Fourth Industrial Revolution" and largely focused on the broad set of issues that impacted economies, governments and firms in the new "digital" age. The subject of technology-enabled innovations permeated many discussions, especially those that focused on the value creation and growth opportunities.

Example

As an illustration of the technology-enabled innovation agenda, I will turn to the transcript from one of the speakers on "The Digital Transformation of Industries" panel at the WEF 2016 conference, Jean-Pascal Tricoire, who is Chairman and Chief Executive Officer, Schneider Electric SA. Mr. Tricoire described the impact of digitization on energy and automation, and how his company leverages these opportunities.

…Energy, invented more than one century ago, is very much siloed: generation, transformation and distribution and consumption (demand). A lot of it is very dis-coordinated with massive inefficiencies.

…In a nutshell – [with digitization] all products will be connected, all the data is getting aggregated, and we deploy analytics to automate decisions.

…We are changing R&D – it is now 60% software related. We have set up an autonomous division.

…[We are] changing relationships with customers. Used to be – projects and services on demand… Now, we stay connected to our customers 24x7, which means we bring new value and new capabilities, and a lot of new services.

…A lot of business is still based on intermediation – you are a "wall" between a customer and a supplier. Now with data, which is shared with our partners, it's changing and opening new ways of working with our partners.

…When you go into digitization… you can't do everything alone. This world is really prone to a lot of partnerships. The big bets you have to make are to choose the right partners.

…The biggest change has been our positioning. Used to be known for safety, reliability and quality. We will continue to be known for this. Now, because it's digital, our customers are calling us for cost optimization, process optimization, predictive maintenance, asset management, which all come natively as a by-product of these systems.

These changes have really been creating new value for our company.

…Transforming R&D is quite a challenge. People are very committed and very smart, but they have very deep skill sets, and it's hard to get them to sometimes see the world from a different angle.

…Question - Now that 60% of R&D is in software, how did you make that transition in R&D happen? It fundamentally changes the way you make the product. In the world before, you make a spec and you spend 2-3 years developing it. Now, you go fast into the market with a minimum viable product and then you can download software to bring more functionality so you are much faster testing the functionality with your customer and much faster adopting the product.

Mr. Tricoire described the new way of doing business enabled by technology, the corresponding value creation opportunities and the related challenges. Interestingly enough, his figure of 60% of R&D being related to software is very much in line with the finding of our survey, with an average of 62% of innovations being enabled by technology.

Impact of cyber-security control processes

Types of impact

Next, I examined the impact that cyber-security related activities are having on these innovative projects. The impact analysis will fall into four main categories:

- Percentage of technology-enabled projects delayed due to cyber-security concerns;
- Percentage of technology-enabled projects cancelled due to cyber-security concerns;
- Percentage of technology-enabled projects with reduced scope due to cyber-security concerns;
- Overall project impact, which is calculated as a "minimum percentage of projects" affected.

Each of the innovation projects can be impacted in multiple ways. For example, if cyber-security is addressed too late in the process, a project may get delayed, it may have changed scope or even get cancelled. Often times, delays and scope changes affect the same project. Therefore, I asked these three questions separately, and then used the largest reported impact for a company as the metric representing the "overall impact" for that company. For instance, if a company had 20% of their projects impacted by delays, 30% of their projects impacted in scope and 10% of their projects impacted by cancellations, I assumed that at least 30% of their projects were impacted overall. In actuality, the number could have been even higher, so this assumption is the most conservative. To examine the impact in these categories, the following question was posed:

Table 8 – impact of cyber-security concerns

Impact of cyber-security concerns

Of all of the technology-enabled projects, in the last twelve months, to the best of your knowledge, what percentage was impacted by either real or perceived concerns of cyber-risks?

Example of such impact
A bank has launched a mobile application for their customers on the IOS / I-Phone platform, but has delayed the release of an Android version of the application for three years due to concerns over the cyber-security of that platform.

#	Answer	Min Value	Max Value	Average Value	Standard Deviation	Responses
1	Percentage of all projects delayed due to cyber security	0.00	90.00	24.04	24.08	57
2	Percentage of all projects cancelled due to cyber security	0.00	66.00	14.19	19.69	31

3	Percentage of all projects where scope was reduced due to cyber security concerns	0.00	75.00	23.96	22.98	45

Number of responses is different because not all companies experienced all types of impact or were aware of it, and some have chosen to only provide numbers for the types of impact they were aware of.

Below are the histograms visually demonstrating the spread of the responses.

Figure 10 – Percentage of projects delayed

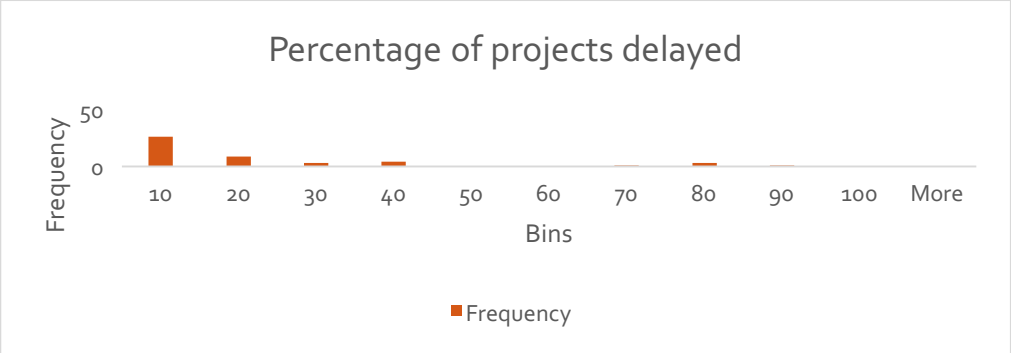


Figure 11 – Percentage of projects cancelled

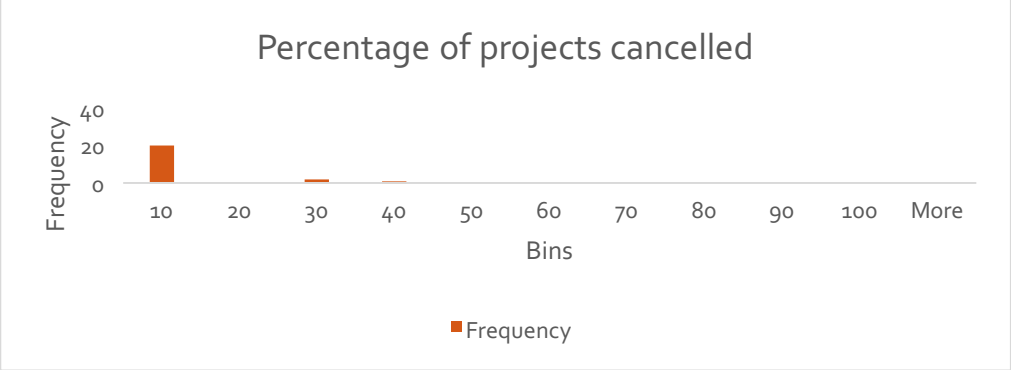


Figure 12 – Percentage of projects with reduced scope

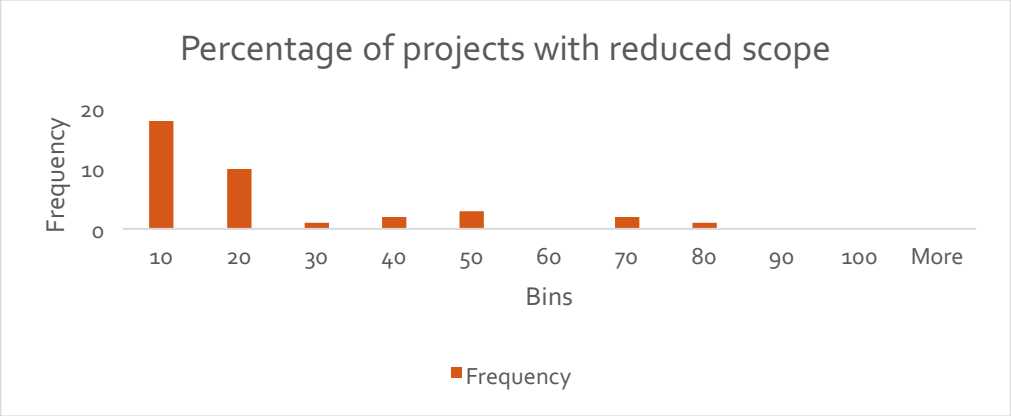


Figure 13 – Overall impact of cyber-security controls on technology-enabled innovation projects

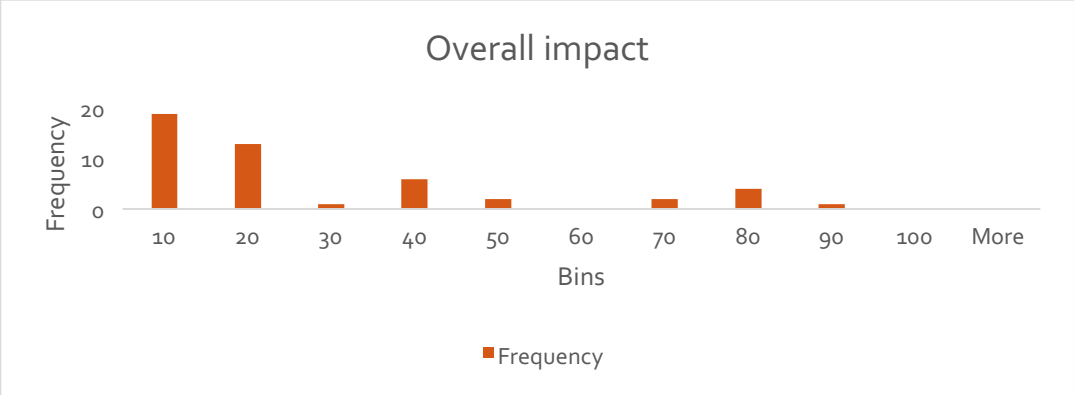


Figure 13 demonstrates the overall minimum level of impact for all companies: as stated above, for each company this is the category (delays, cancellations, scope changes) they noted as having the largest stated impact. Based on the results of the survey, we see that the majority of the negative impact on projects comes from delays and scope changes, as required by the cyber-security related control processes, and very few are related to actual cancellations.

When looking at the overall impact, we notice three clusters of impact:

- A group with very low impact (20% of projects or lower are impacted);
- A group with medium impact (20% - 50% of projects are impacted);

- A group with high impact (above 50% of projects are impacted, with 70% - 90% being the most common occurrence).

The most common types of such negative impacts are delays and scope reductions, with cancellations being a rare occurrence.

In addition to this quantified data, we asked our respondents to provide us examples from both ends of the spectrum: on the one hand, when in their opinion company has taken on too much cyber-risk, and on the other hand, when company was excessively risk-adverse and didn't take advantage of the innovation opportunities. Here is the exact phrasing of the question, results of the responses and examples provided. Only 19 of the 54 companies surveyed answered this question.

Reading through these answers, it became clear that the examples fell into three distinct categories, which were then tabulated and represented in Table 9. These categories are:

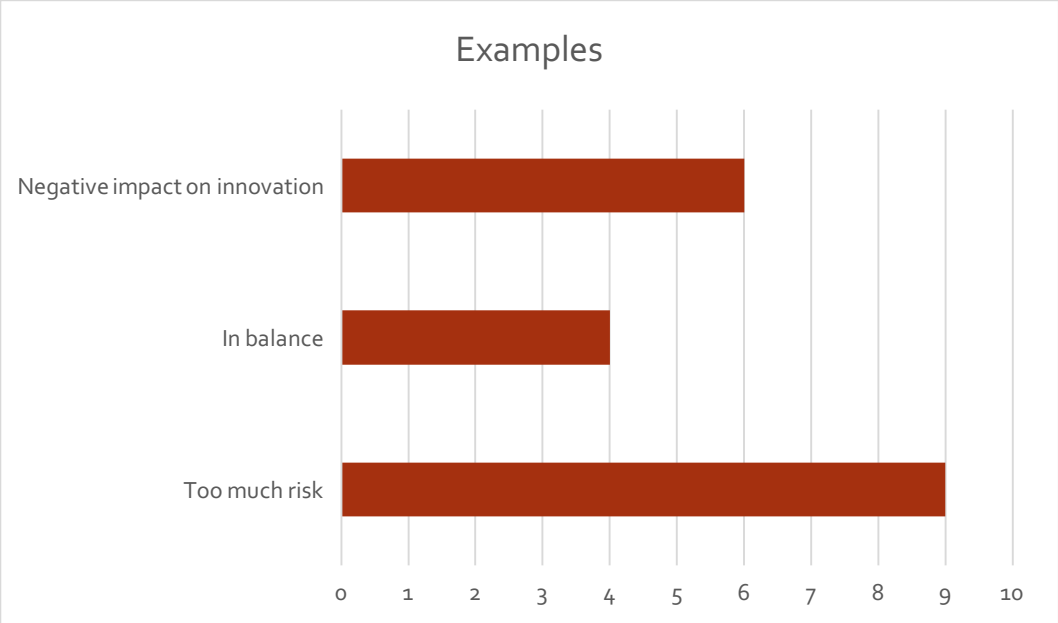
- Negative impact on innovation: these respondents provided an example where strong cyber security came at the expense of innovation, creating tensions and perceptions of reduced value; specific answers in this category are shown in Table 10;
- In balance: these respondents provided a few examples where innovation and cyber-security efforts were well balanced; specific answers in this category are shown in Table 11; example of patient portal is especially illustrative;
- Too much risk: these respondents felt that the company was taking on too much risk in order to achieve their innovation objectives, thus creating a certain amount of tension; specific answers in this category are shown in Table 12.

Table 9 – Examples of organizational issues and tensions caused by cyber-security and technology-enabled innovation

Organizational characteristics associated with achieving the satisfactory balance of technology-enabled innovation and cyber-security efforts

Please describe any organizational or structural tensions, challenges, support networks or alliances that exist when addressing decisions on technology enabled innovations and corresponding cyber-risk analysis.

Examples
IT infrastructure and Operations IT teams have different priorities
Projects get approved by various business disciplines without consulting with the IT Security team, causing delays, scope increases within projects or increased costs
IT security team is short on resources



The examples provided can be characterized as follows.

Examples of the negative impact on innovation

Table 10 – Examples of the negative impact on innovation

My company has capacity to gain customer's activity through online. But it is always blocked or stopped due to legal risk. Actually, we have many kind of opinions to deal with customer's information, and no one knows clearly.
We'd like to share information into cloud storage, but we're afraid of the risk, we can't do it until now.
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.
CAPTCHA's and two-factor authentication are becoming more widely recognized forms of ensuring account security but they appear as a hinderance to customers from the businesses perspective. They have caused delays as we work to reach agreement and ensure that they are meeting brand requirements.
My organization falls under both the "too much" and "not enough" categories. Under "not enough" we've had applications attacked from China, and yet NONE of the security assessments address hacking. Under "too much" is the process in which threats are obvious to the delivery team, but take time to perform the assessment.
Huge opportunity in building and leveraging deep customer insight in more analytical and data driven decision processes. But not allowed to consolidate client data due to governmental regulations. Also - huge opportunity in leveraging public cloud offerings. But still not allowed due to governmental regulations.

Examples of a well balanced approach

Table 11 – Examples of a well balanced approach

We have few examples of this in the last two years, but previous to that it was common to complete projects before cyber security requirements were addressed. The only remaining area of concern is I.T.-driven infrastructure projects, which operate without clear customers and sometimes still minimize security.
We reduced (contained) the scope of data in our BI toolset specifically to ensure that data is not inadvertently leaked while doing analysis.
We had none of such issues till date, as cyber security is viewed with utmost importance and hence no project goes through without enough oversight within the group.

Process of provisioning access to a patient portal access was cumbersome due to perceived high risk of giving an account to someone who is not the patient. Worked with Legal to come up with a process that was more streamlined that took on a little more risk but was in line with other established processes of identity verification. The benefit was that more patients were likely to follow through on the process of getting their account and thus would benefit from all of the information and efficiencies from the platform when managing their own care.

Examples of too much risk

Table 12 – Examples of too much innovation focus at the expense of cyber-risk exposure

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.
Most of internet company I know of, including this one, emphasize innovation speed, iterations with failures. In that context, cyber risk prevention is something that are put in place to support, not to stop any new projects.
The business units are planning to offer sales people mobile devices to enhance them to deliver services out of office and boost the sales. However, it would violate the current principles of cyber security and customers' data protection. So, the sales division and IT team argue each other severely.
Cyber security is given lip service but no projects are side lined or delayed due to check for potential cyber risk
I think a lot of the risk that we didn't pay attention to properly was more around an employees ability to capture and send customer information outside our network via their personal e-mail, cell phones that could take pictures of their screens, etc.
My organization falls under both the "too much" and "not enough" categories. Under "not enough" we've had applications attacked from China, and yet NONE of the security assessments address hacking. Under "too much" is the process in which threats are obvious to the delivery team, but take time to perform the assessment.
We had a client that had a large app deploy that had some certificate encryption related issues. Chrome and other browsers would throw a Diffie-Hellman key error,

they decided to launch with this key issue despite the display issue knowing they would update later. This left us exposed and advertised the issue to the client.
My division has just reached to the $1 Billion revenue last year and it means that the business volume has entered to the different stage at which the cyber risk shall be taken more seriously. However, it would be challenging will take some time to change the culture and management's thinking of raising the priority on the cyber-risk.
The competitor company has an example. The collection of customer information for 10 million people was revealed outside as the cd-rom was sold to the information broker, and it was reported in local news. Though it was a big issue, it has been forgotten soon because there were many similar issues in credit card company or bank.

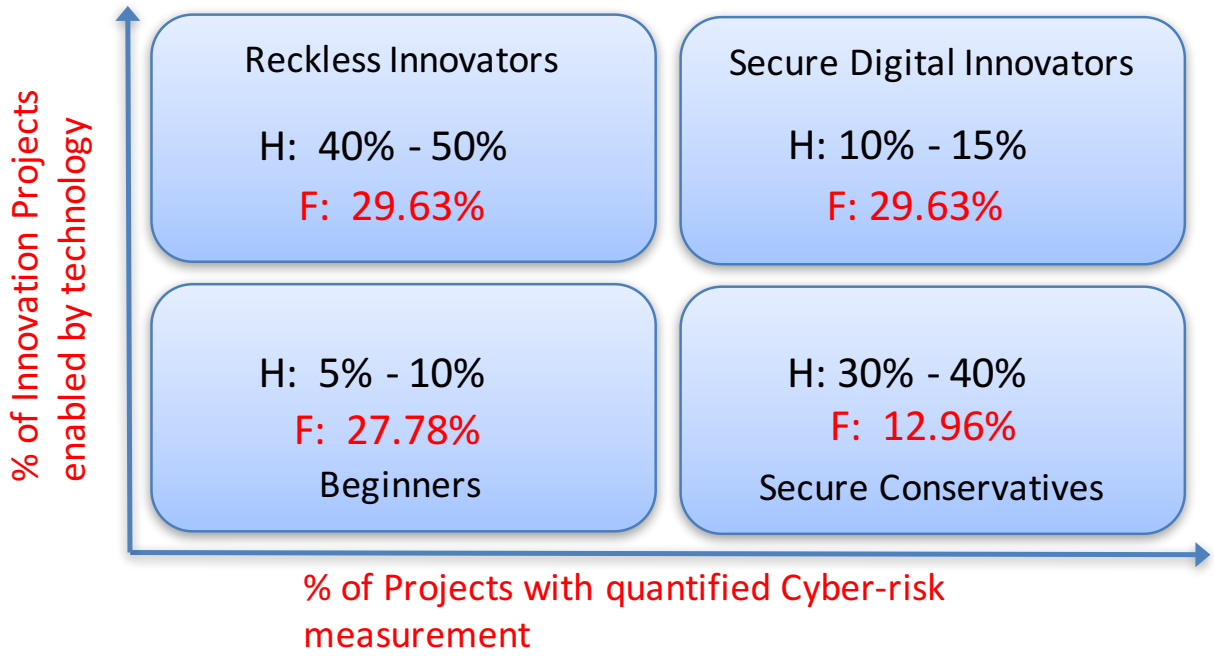
Relationship between level of innovation, cyber-risk measurement and the impact of cyber-security controls

Finally, and most importantly, I wanted to see how the three dimensions were connected, utilizing the originally envisioned framework. While the data from 54 surveys cannot provide statistically accurate results, it was my hope to at least establish a pattern that could then be examined in more detail through the interviews. Here are the most pertinent findings.

First, I took a look at the number of companies in each quadrant to test my original hypothesis. Here are the results, which are demonstrated graphically in Figure 14:

- 27.78% of companies came in "below average" on both the "Technology Innovations" as well as "Cyber Security Maturity" measurements; my hypothesis for this quadrant was 5% - 10%;
- 12.96% of companies came in "below average" on the "Technology Innovations", but above average on the "Cyber Security Maturity" measurements; my hypothesis for this quadrant was 30% - 40%;
- 29.63% of companies came in "above average" on the "Technology Innovations", but below average on the "Cyber Security Maturity" measurements; my hypothesis for this quadrant was 40% - 50%;
- 29.63% of companies came in "above average" on both the "Technology Innovations" and on the "Cyber Security Maturity" measurements; my hypothesis for this quadrant was 10% - 15%.

Figure 14 – Results of hypothesis testing using the original framework



Second, I evolved my originally envisioned framework in the following ways:

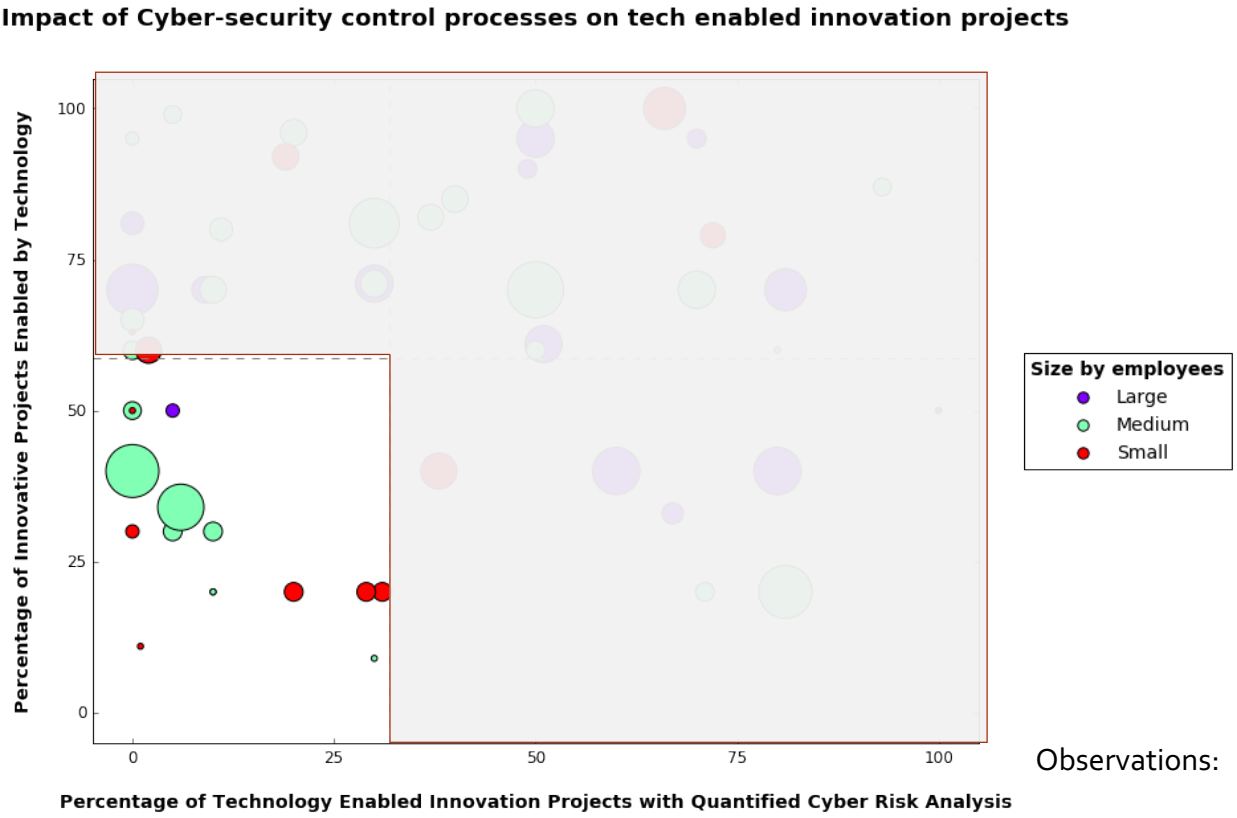
- It turns out that for each quadrant of the framework, there is a set of good reasons for why certain companies may find themselves there; therefore, I removed all of the labels that might carry negative connotation or simply be inaccurate;
- I utilized averages as the dividing lines, which means that over time quadrants will shift, and companies might easily shift from one quadrant to another;
- I added the "size of the bubble" as the third dimension, to represent the negative feedback that an organization experiences due to cyber-security controls;
- I added a colour dimension to help visualize various metadata, such as size of the company, region of the world and the industry.

Finally, to properly examine the dynamics within the model, I utilized the quadrant-by-quadrant analysis. As a reminder the X and Y axes represent the following:

- The X axis measures the maturity of cyber-security within an organization;
- The Y axis measures to what extent an organization depends on technologies to execute their value creating innovation agenda.

1st Quadrant

Figure 15 – 1st Quadrant: Impact of cyber-security control processes on technology enabled innovation projects



Observations:

In the first quadrant, companies' reliance on technology for innovations is below average, and their measurement of cyber-risk is below average. Not surprisingly, most companies in this quadrant are small and medium in size, with one exception. Most companies (with two exceptions) also experience minimal impact from cyber-security controls.

Why would companies find themselves in this quadrant?

- This is a good place for many start-ups, as they are just trying to build up their company and don't have the luxury of a traditional large firm to fully address all of the risks, cyber-risk among them. At first, one assumes that the start-ups will have a high percentage of innovative projects, but upon further examination it becomes clear that start-ups are only working on a very small number of projects at a given time, due to constrained resources. Even high tech start-ups may only have one project that is actually high tech, their original idea. The rest of the projects in the early years are marketing, financial, and operational to get that idea to market. As the company grows and product develops, things will change. As a company is planning to exit,

either through an IPO or an acquisition, cyber-risk is likely to surface in the due diligence process. Also as start-ups grow and evolve, they start taking on new projects, and potentially would move into another quadrant, especially on the Y axis;

- Small and large companies with diversified or federated business models, operating as a collection of small businesses, are also likely to fall into this quadrant;
- Companies that don't have a lot of technology needs, beyond just very basic utility technologies, may also comfortably be in this quadrant, although in today's day and age it is hard to find such companies.

The following three quotes from my interviews and survey comments provide a good illustration of the types of companies that can be found in this 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 choose their own platform, implementing security measures was the #1 impairment. Cross-divisional innovations will happen after we establish centralized IT utility and address security."

Energy start-up:

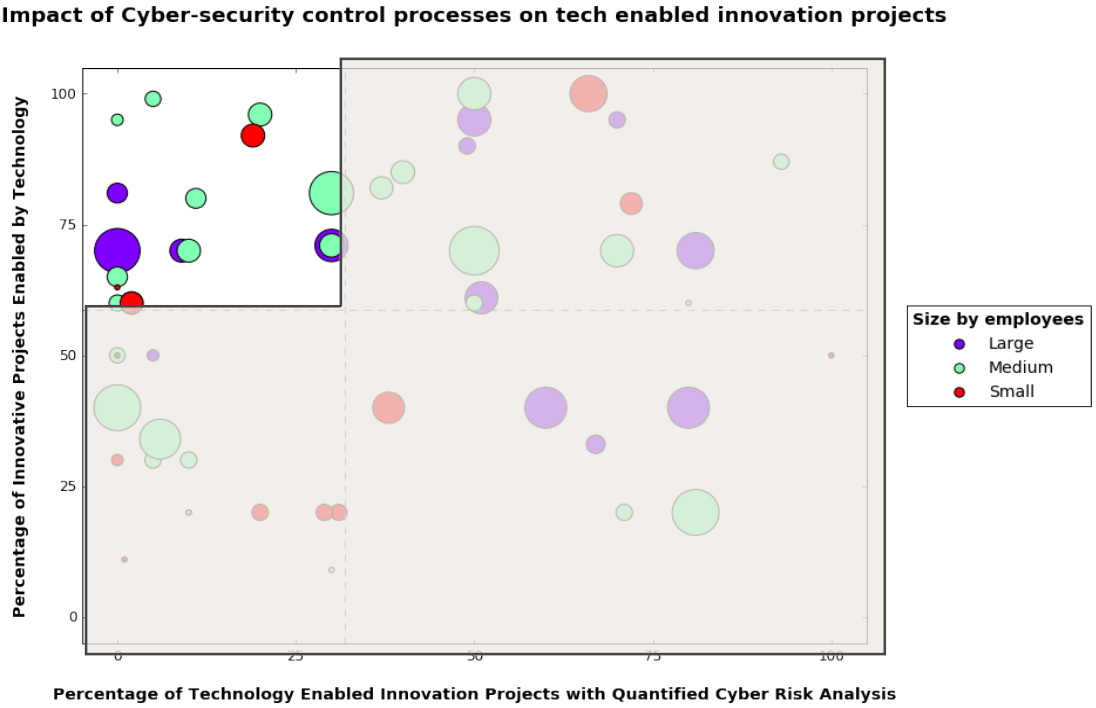
> "We are a startup engaging in renewable energy business. At the moment, we spend quite little time on cyber-risk analysis."

Venture capital firm that invests in technology start-ups:

> "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 exit due diligence".

2nd Quadrant

Figure 16 – 2nd Quadrant: Impact of cyber-security control processes on technology enabled



In the second quadrant, companies' reliance on technology for innovations is above average, and their measurement of cyber-risk is below average. This quadrant has mostly medium size companies, with four large ones and three small ones. With a couple of exceptions, negative impact on projects from cyber-risk controls is quite low. Since technology enabled innovations are above average and risk is not measured (thus is likely not understood), it is possible that some of these companies are building in a degree of risk that they may not be fully aware of.

What kind of companies would companies find themselves in this quadrant?

- Growing start-ups and medium companies that are expanding through technological innovation may find themselves in this quadrant;
- Companies with high competitive pressures to innovate are either in this quadrant or in the fourth quadrant;
- These companies rarely measure cyber-risk, while heavily relying on technology for the innovations; this could be explained by a variety of reasons:
    - They are implicitly accepting higher levels of risk, and are prepared to deal with the consequences;
    - Technologies and/or datasets that are being built out may have very little value to potential attackers, and thus are by definition have low risk of cyber threats;

- Companies may not fully understand that they are taking on risks. In fact, according to the interviews, there are some companies where at the board level there is a desire to address the risk, but at the middle management level, due to a number of management practices later described in this document, risk is not being properly addressed as new technology is being built out.

The following two quotes from my interviews and survey comments provide a good illustration of the types of companies that can be found in this quadrant.

Small Industrial Electronics and Electrical Equipment

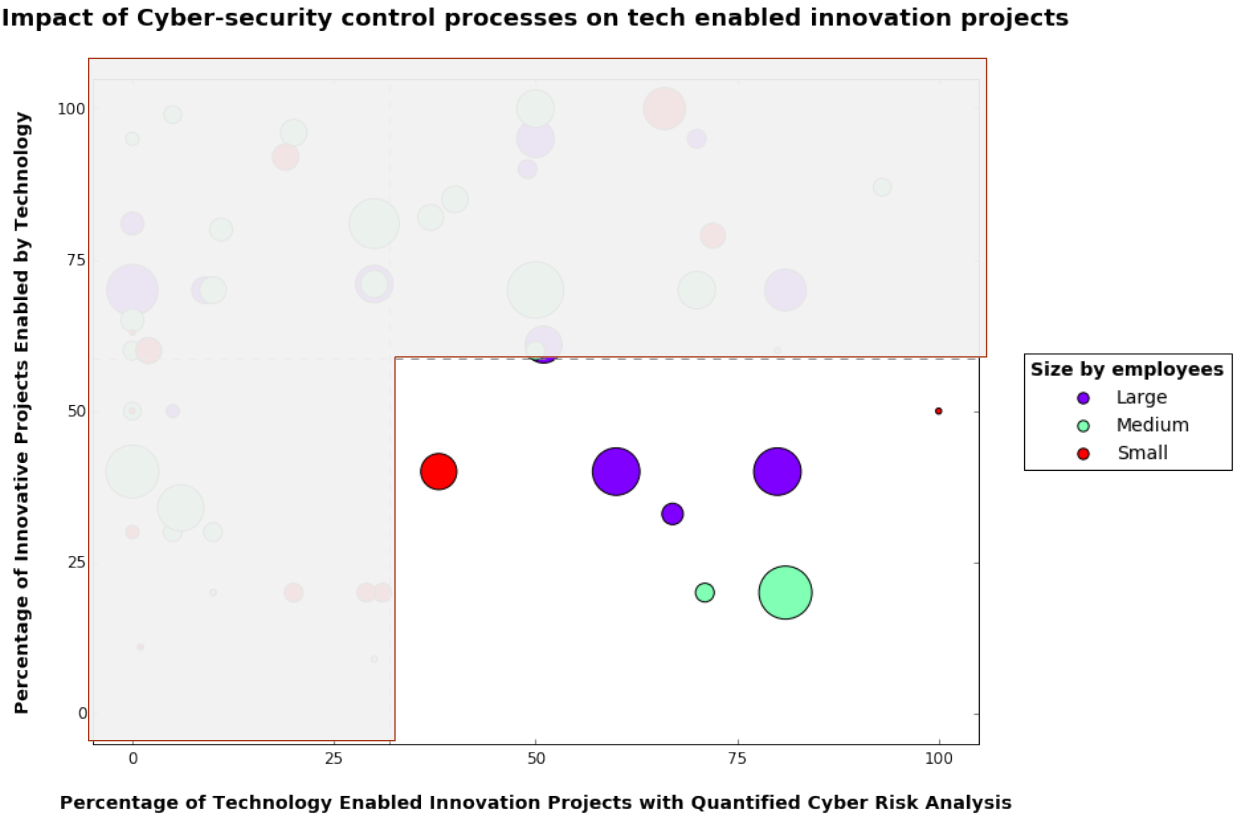
> "Although recognized as a potential threat to the well-being of the organization, the inability to quantify the degree of the damage allows management the luxury of delaying adequate deployment of resources."

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

Figure 17 – 3rd Quadrant: Impact of cyber-security control processes on technology enabled innovation projects



In the third quadrant, companies' reliance on technology for innovations is below average, and their measurement of cyber-risk is above average. Companies of all sizes are equally represented in this quadrant. This quadrant has the least number of companies as compared to others (13%). Negative impact is split – three companies have large negative impact, three companies have relatively low negative impact and one is in the middle. Companies in this quadrant may be losing out on the opportunities to achieve competitive advantage through technology, although not necessarily: this will largely be dependent on their industry and competitive landscape.

What kind of companies would companies find themselves in this quadrant?

- Many companies are in the industries where competitive pressures are not as high and they don't feel as much pressure, while at the same time there is low appetite for cyber-events and adequate focus and resources on measuring and management of cyber-risk;

- Some companies (i.e. a nuclear power plant) intentionally establish a "slow follower" strategy as a way to ensure that only well tested, previously implemented technologies are selected.

The following two quotes from my interviews and survey comments provide a good illustration of the types of companies that can be found in this quadrant.

Government contractor

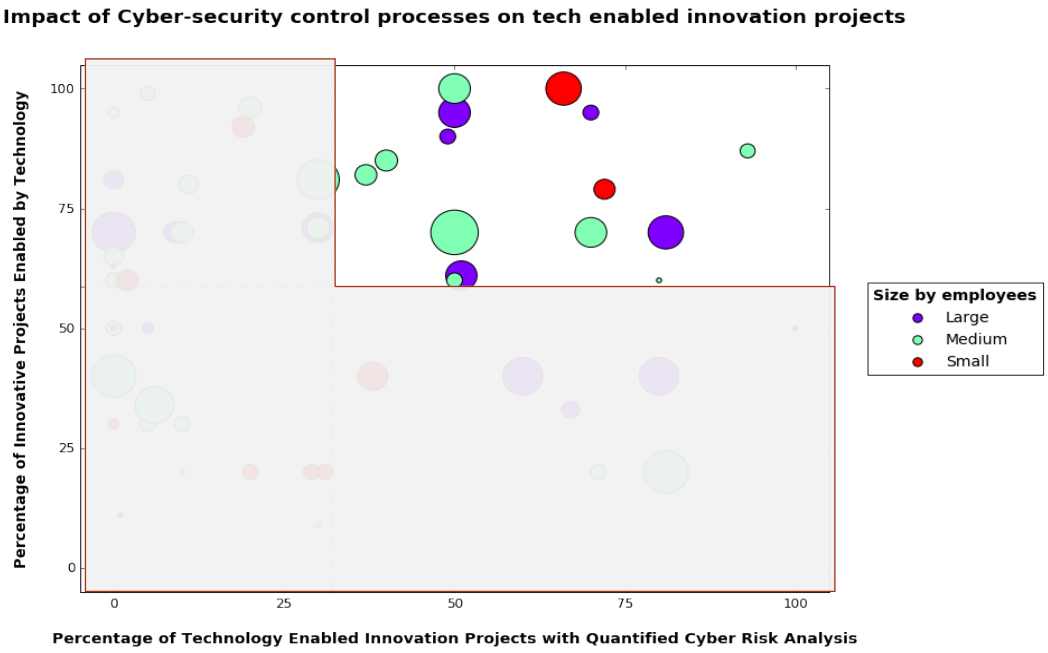
> "Poor alignment between field operations and centralized Cyber Security Unit. Also poor digital maturity and risk awareness in senior business leadership. Result: Fairly strict and conservative cyber security policy and practice. Opportunities are lost due to conservative security policies and lack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

4th Quadrant

Figure 18 – 4th Quadrant: Impact of cyber-security control processes on technology enabled innovation projects



The 4th quadrant consists primarily of the medium and large firms, plus two small firms. In the fourth quadrant, companies' reliance on technology for innovations is above average, and their measurement of cyber-risk is above average. What is also very interesting is that here we have both companies that experience high negative impact from cyber-security control processes, and those that experience little negative impact.

Why would companies find themselves in this quadrant?

- Many companies are either in this quadrant or aspire to be in this quadrant;
- Companies with high competitive pressures to innovate are either in this quadrant or in the second quadrant;
- All of these companies acknowledge the necessity to mitigate cyber-risk as they build out their digital capabilities.

The following two quotes from my interviews and survey comments provide good illustration of the types of companies that can be found in this 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

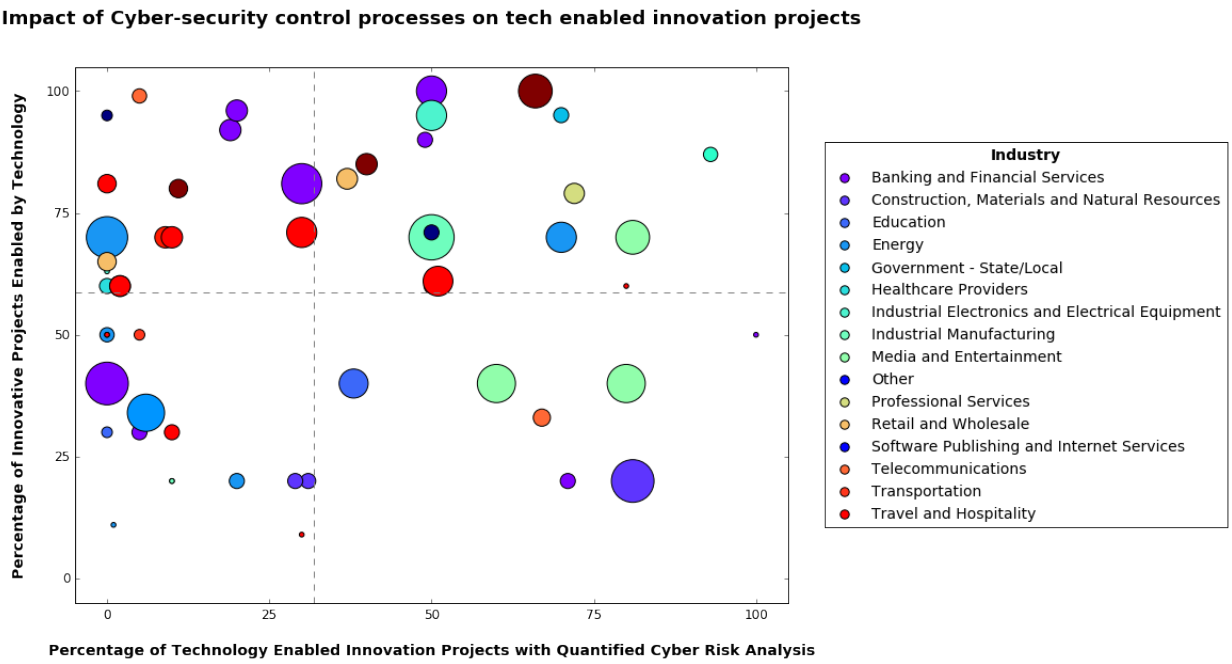
> "The company is very conservative and cyber-security is an audit committee board level interest. When Target happened and their CEO was fired, our CEO announced that PCI compliance of our product is our #1 priority. People hated it – investment was large and cut-out a huge number of possible projects. 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 cyber-security can accelerate innovation."

Key factor analysis

Comparison by industry

Surprisingly, there was a lack of clear pattern in the industry analysis, although it is possible that some patterns might have become evident with a larger data sample.

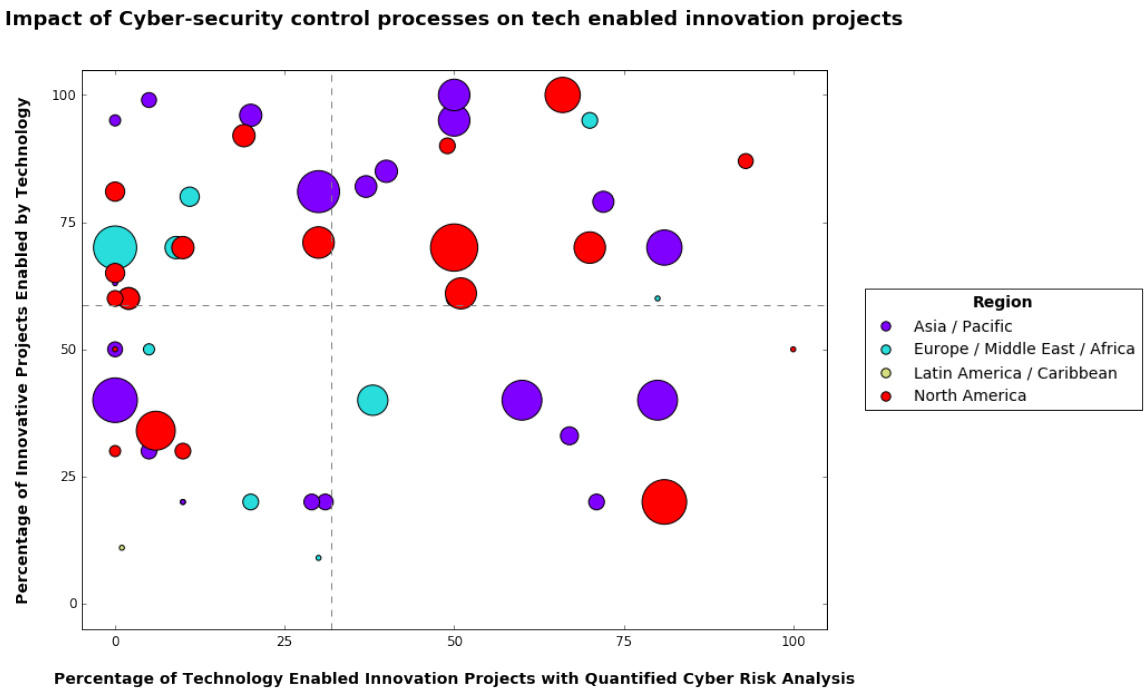
Figure 19 – Industry comparison



Comparison by region

Looking at the data on a regional basis shows a lot more rigor and emphasis on risk measurement from the firms located in the Asia-Pacific region. The North American region doesn't demonstrate a pattern, and the Europe/ Middle East / Africa region trails behind others in terms of both cyber-risk measurement and the impact, although EAME sample size is too small to make this conclusion definitive.

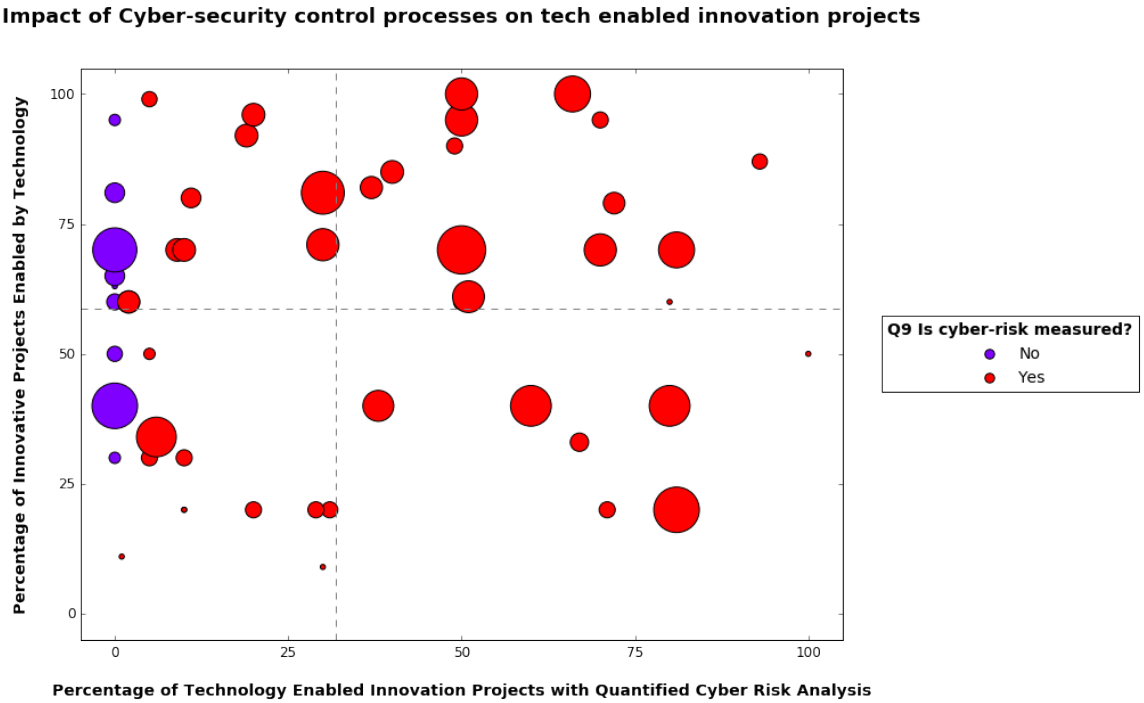
Figure 20 – Region comparison



Comparison by whether cyber-risk is measured or not

Perhaps the most interesting finding was that of simply comparing firms that measure cyber-risk, vs. those that don't. It appears that firms, with two exceptions, that don't measure cyber-risk don't experience a lot of impact on innovation, and vice versa.

Figure 21 – Comparison by measurement / Yes or No



Looking at Figure 21, we can see that there are two companies that are located on the zero line on the X axis, but have a large negative impact associated with cyber security processes. Most likely, these two companies are regulated in terms of cyber-security and therefore experience negative impact, however, simply don't measure cyber risk. Most of the companies that we find below average on cyber risk measurement experience relatively low negative impact.

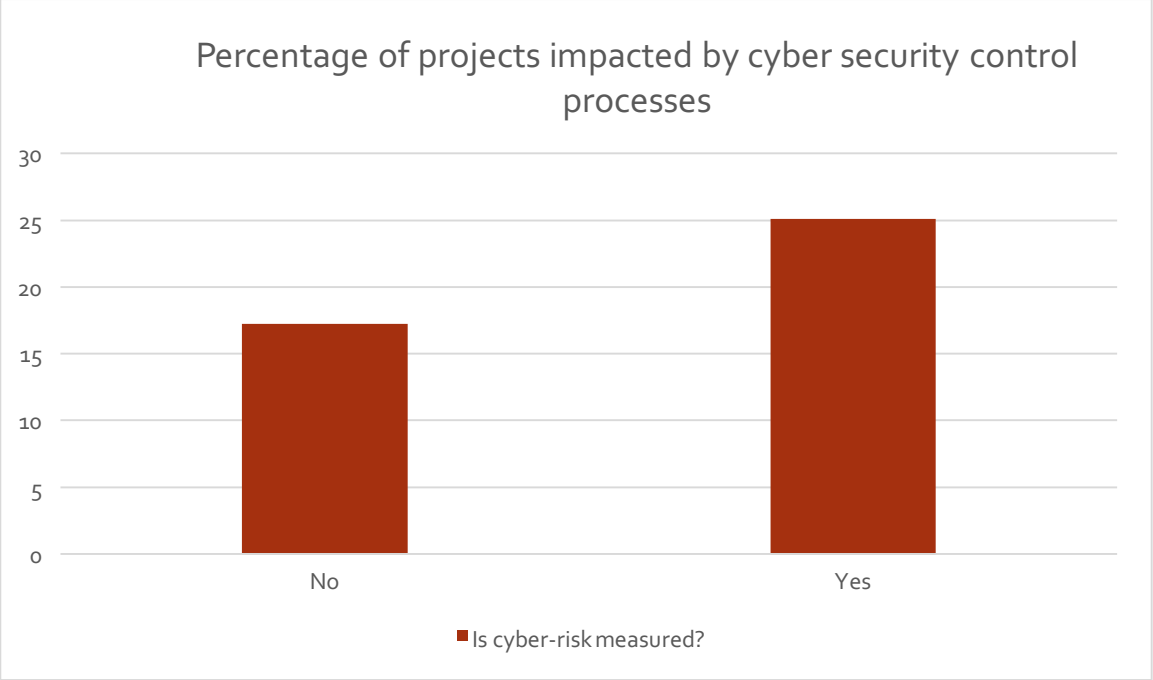
As we move along the X axis, we can see that more and more companies are experiencing higher levels of negative impact associated with cyber risk measurement. This is not at all surprising as we would expect that cyber risk measurement efforts lead to a more thorough understanding of the risk, and result in more activities that could potentially lead to or be perceived as having a negative impact on innovation.

. What's even more intriguing is that several companies with above-average cyber-risk measurement practices experience little to no impact on their technology-enabled innovation projects. What could be the reasons, and how are these companies different from those that put a lot of emphasis on the measurement and experience increased levels of impact? Here are some possible hypotheses that I wanted to explore through the interview process:

- Perhaps, following the cyber-risk / benefit analysis, companies are deciding to go ahead and accept a certain amount of risk and therefore experience low impact;
- Perhaps, some of these companies successfully established a very efficient R&D process that minimizes the impact of cyber-risk without compromising their security posture;
- Perhaps, a certain amount of delays and scope changes are "baked" into the project scope from the very beginning and is considered a part of the whole.

The answers to these questions will be explored in the following chapters based on the interviews. For now, to further quantify this relationship, I calculated the averages.

Figure 22 – Percentage of projects impacted by cyber security control process, by measurement



Although we cannot establish the causality of this relationship, we can see that the relationship does exist. Therefore, it is reasonable to turn to the qualitative approach to further understand the aspects of this relationship. As such, I collated the comments about "Organizational characteristics" that relate to achieving this balance. Here is the question as it was asked, and the analysis of collated responses.

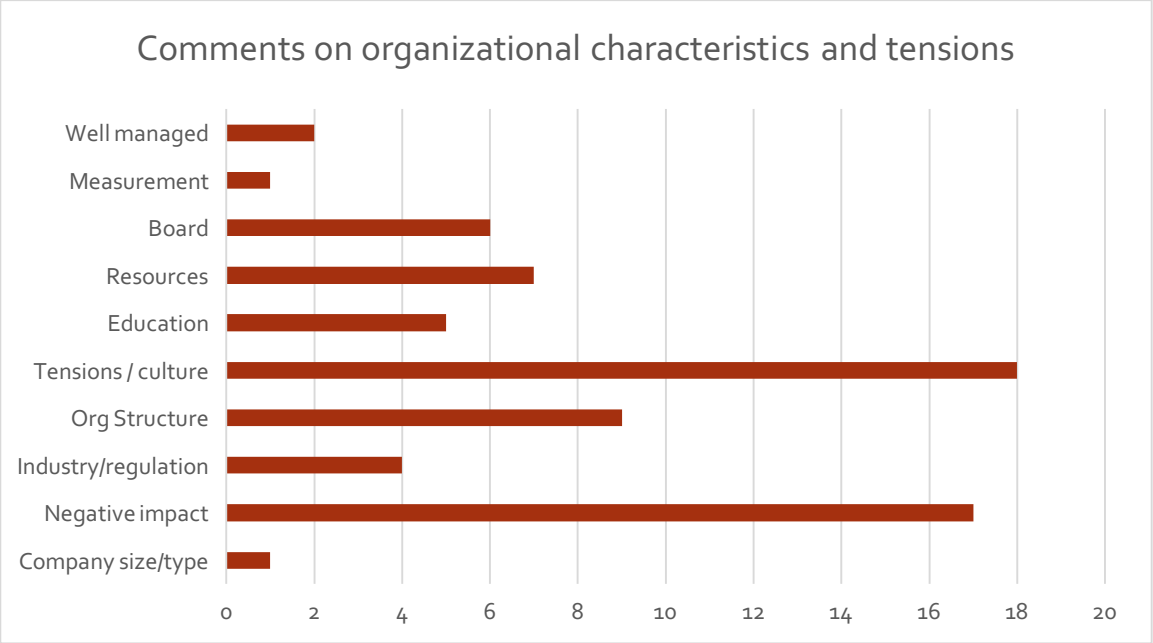
Clues to finding additional factors impacting the balance

I took all of the comments in the "organizational characteristics and tensions" question of the survey, and tabulated them by common categories, allowing each comment to be associated with multiple categories as appropriate.

Figure 23 simply represents the number of comments that survey respondents provided in relation to a particular topic (for example, 9 respondents highlighted organizational structure in their description of organizational characteristics related to achieving the balance). These categories can be defined as follows:

- "Well managed" represents responses where respondents felt that both the innovation efforts and the cyber-security efforts were well balanced and well managed;
- "Measurement" represents the responses that touched on cyber-risk measurement being associated with achieving a satisfactory balance between technology-enabled innovation and cyber-security efforts;
- "Board" represents the responses that mentioned boards of directors and their role in achieving a satisfactory balance between technology-enabled innovation and cyber-security efforts;
- "Resources" represents the responses that mentioned resources, either funding or talent, as factors in achieving the satisfactory balance between technology-enabled innovation and cyber-security efforts;
- "Education" represents the responses that mentioned education and awareness in any part of the organization as factors in achieving the satisfactory balance between technology-enabled innovation and cyber-security efforts;
- "Tensions / culture" represents the responses that pointed to company culture or spoke of organizational tensions as factors in achieving the satisfactory balance between technology-enabled innovation and cyber-security efforts;
- "Org structure" represents the responses that pointed to organizational structure and reporting lines as factors in achieving the satisfactory balance between technology-enabled innovation and cyber-security efforts;
- "Industry/regulation" represents the responses that pointed to either industry impacts or regulatory pressures as factors in achieving the satisfactory balance between technology-enabled innovation and cyber-security efforts;
- "Negative impact" simply identifies those responses where the company was negatively impacted, in any way, by the tensions associated with achieving a satisfactory balance between technology-enabled innovation and cyber-security efforts;
- "Company size/type" represents comments where respondents felt that the type or the size of their company was a factor in achieving a satisfactory balance between technology-enabled innovation and cyber-security efforts.

Figure 23 – categories of comments on organizational characteristics and tensions



Details of all of the comments can be found in the Appendix. In the meantime, I will further drill down into those categories, to help explain the complexity of achieving the balance between technology-enabled innovation and cyber-security.

Chapter 4: Industry impacts

To evaluate industry impact on the technology-enabled innovations and cyber-security trade-offs, I will examine the learnings from the interviews in the area of regulatory compliance, innovation pressures / digitization and history of breaches.

Regulatory compliance

Types of regulatory compliance

One of the factors impacting the cyber-security agenda and innovation is the regulatory environment, specifically, cyber-security regulations. Based on the interviews, some of the strongest regulatory impact was observed in companies that have to comply with the highest levels of Payment Card Industry standards (PCI) and with Financial Services regulations. In fact, for companies where PCI is the only cyber-security related regulation, their entire cyber-security team and all of their budget is driven by PCI requirements. Furthermore, the PCI framework provides them with the foundation for security measurements, KPIs and reporting to the board. It is important that in these companies security is looked at from a broader perspective, well beyond PCI, to identify other areas of risk and exposure, even if ultimately the work is folded into the same security organization. This approach should protect companies from having a too narrow, PCI-only, view. . For example, if a company regulated by PCI also has to protect its highly valuable intellectual property, highly sensitive customer data or complex sensor systems that could be of interest to a state actor, then the PCI compliance framework will not be sufficient for their business purposes. It is, in fact, a critical responsibility of the IT Governance team to constantly examine the risks, and ensure that the best suited framework or frameworks are used.

Some PCI regulated companies understand that PCI is only the compliance part of it, and that actual security goes far beyond compliance. However, they find it quite efficient to use PCI for communications, reporting and budgeting purposes, and not to separate additional security efforts into their own category.

PCI compliance is mandatory, and penalties and liabilities for fraud are imposed on large merchants for any non-compliance, although small merchants with self-attestation don't have to pay penalties. Additionally, PCI compliance has to be re-evaluated fully on an annual basis, and incrementally on a quarterly basis, focusing on the changes in the computing environment and re-establishing the perimeter. These factors make PCI a really powerful and real tool that cyber-security teams in large enterprises can use to drive forward their agenda, and create awareness not only at the senior level, but also throughout the organization.

In terms of the innovation agenda, PCI regulated companies are also the ones that innovate in the payment technologies areas. Awareness of cyber-security related matters and relative maturity in this segment empowers firms to push forward and continuously accept greater numbers of payment methods from their customers.

In terms of other innovations, many companies that have truly achieved 100% PCI compliance and managed to sustain this compliance from year to year, have also developed a clear approach to ensuring that all newly developed technologies go through security architecture review early on in the process, and get evaluated on a regular basis and prior to release, before being incorporated into a regular change management cycle. Since quarterly and annual PCI reviews are mandated and look at all the changes in the computing environment, this process naturally forces the companies to adopt their policies and procedures to have all of their new technologies be ready for review. If such review doesn't pass the security tests, it goes back for modification until a passing grade can be achieved. Thus, the innovation process is quite robust and well understood.

When mature organization awareness is combined with board support and measurement, impact on innovation is lessened. When PCI compliance is measured by the business unit, and such KPIs are reviewed by the senior management and the board, business units are naturally inclined to very quickly come to the security team with all of their new technology based projects. If one of these factors is not present, however, the impact increases as more and more projects get too late into the development cycle before security issues are addressed. An additional proof of maturity of the PCI-based cyber-security approach is its involvement with the supply chain partners, and the practice of holding them up to the same standards. This is a relatively recent development in the PCI compliance framework, and many debates are still on-going with respect to its robustness and practicality.

In addition, a very interesting regulation is coming out of Europe. Although this is more of a Data Privacy related regulation, it will force companies to disclose any customer data loss and pay large fines, giving consumers more power and imposing more stringent and onerous controls on the companies operating in that region. This new regulation will likely broaden a spectrum of companies that will have to step up their cyber-security efforts.

Some of the other interviewees worked in industries that were subject to multiple regulatory requirements, such as Sarbanes Oxley (which currently has a number of cyber-security related requirements). In addition, some have adopted the NIST framework, and were in the process of mapping various regulation to the NIST framework to ensure a single approach. These companies developed internal security policies that ensured compliance with all necessary regulations.

In contrast, discussion with the companies from non-regulated industries revealed an "uphill" battle problem faced by the cyber-security teams. This problem was amplified in the companies where technologies are the cornerstone of the new value-creation innovation agenda, and the competitive pressures are high. In an environment where lack of mandatory compliance was combined with the lack of organization awareness, competitive pressures to innovate far outpaced any hypothetical risks of cyber threats, consequently leading to a number of ungoverned and untested product releases.

Examples

One such example comes from a worldwide transportation company. They have been achieving PCI compliance for the last few years, and continued to improve their processes. For annual assessment, in addition to all of the reviews and testing, a random number of locations is selected for a site visit, and any gaps are remediated within a firmly prescribed timeline. This evaluation is an annual cycle. On the supply chain side, there are two approaches. First, consider a supplier to be a "part of the family". This means that the supplier must comply with all of the company's policies and procedures, and be included in all of the reviews. The second option is to treat the supplier as a service provider, in which case they are required to do their own annual attestation of compliance, with the right to audit. The only debatable issue is in dealing with those suppliers that choose to do a "self-assessment", and this is where the right to audit becomes very important. For example, there is a third party call center provider in India who chooses to do self-assessments, and annual visits are performed to verify their status. What becomes more complicated, and even unreasonable, is the need to go several "layers" down the chain. This is just too cumbersome and unrealistic. The solution to this issue is to have each party in the chain confirm and attest their own compliance.

With this mature level of assessment, all of their partners, as well as their business units, are measured on PCI compliance levels, and such measurements are frequently and transparently shared with the executive leadership team as well as the board of directors.

This particular transportation company is quite innovative: they have an SOA-based architecture innovation strategy, as well as a strong enterprise mobility effort. The primary innovation driver is customer experience. In fact, there is a separate "innovation" group in the organization, reporting directly to the executive team. The group looks at all innovations, investigating anything that is "new and shiny", to see if it's relevant to the company and can generate additional value creation opportunities. Occasionally, this group "makes pronouncements" on strategies without consulting the security team, and that's when concerns arise; however, this is a rather infrequent occurrence. For example, a few years ago, such a pronouncement caused the firm to quickly move to the cloud-based Office 365,

enabling all of the "cool" features that are available. One such cool feature was employees' ability to link their Office 365 and personal OneDrive, to make working from home an easier process. Soon after the implementation, it became apparent that home-based computers are shared with other family members, have loose passwords or no passwords at all. Upon discovery by the security team, this feature was turned off.

Another example was the Enterprise Mobility implementation, where iPADs were quickly distributed not only to the office workers, but also to the front line employees. In this new application, some of the customer data was stored locally on the iPAD, and the innovation team had not considered what would happen should one of these iPADs get lost. Shortly after the release, security team had to go back and address the design of this solution to comply with all of the security policies and standards.

These two examples demonstrate that even in the mature cyber-security organizations, with measurement, support and broad awareness, incidents of insecure design still happen. Luckily, the regulatory framework allows the security team to catch and quickly address these concerns, although it requires certain features to be turned off and not all of the planned benefits of the innovations to be released.

Summary of the insights

- Cyber-security regulations that impose penalty and require frequent assessments help shape mature cyber-security organizations that can promptly address security issues in any new technology-enabled innovations;
- Once a certain level of maturity is achieved, in well managed organizations that can be considered as following best practices, compliance focus is replaced with security focus;
- Cyber-security regulation provides a very useful tool to security teams in the early stages, as it allows them to raise the awareness across the organization, gain support from the board of directors, implement compliance measurements and embed security into most new innovations at an early stage; however, the long term impact of cyber-security regulations have not been examined;
- Separate innovation groups can benefit from a more pro-active approach to cyber-security to enhance their estimates of the true value creation and time to market of the new initiatives.

Innovation pressures

As described in the first chapters of this paper and illustrated by the McKinsey's MGI Industry index, a growing number of industries are actively entering the technology-enabled innovation race. For example, in a recent Bloomberg interview, a General Motors executive commented that the company growth strategy largely depends on the innovation around

connected cars, additional technology-enabled passenger safety, and growth from a shared economy play with a major investment in Lyft. The same applies to a number of other companies interviewed, but not all of them.

Here is how I would like to categorize the innovative agendas of the various companies:

- Strategic technology-enabled product innovations;
- Strategic technology-enabled innovations focused on internal processes;
- Tactical technology-enabled innovations at the operating unit level.

Strategic technology-enabled product innovations

This group of technology-enabled innovations covers those efforts that are related directly to product development for the company. For example, for a mobile wallet company, the security of their mobile app will fall into this category. For an IoT company, both the physical device with the sensor, as well as the app that is given to the customer will fall into this category.

In this group, companies were under immense pressure to get their product, either fully digital or with digital elements, out of the door. However, there was quite a spread in the variety of ways to address the security of the products. More specifically, here were the three approaches:

1. Buy a separate cyber-security start-up specializing in the particular product, and keep it completely separate from the rest of the security team. With this approach, the team that was responsible for product design effectively understood and took ownership of the product security as one of the core features. The exact information of the results of this approach is limited, as my interview was with their Enterprise CIO, but suffice it to say, security of the product is being taken very seriously, hence the acquisition.
2. The second approach is to have an internal product-based security team, with the ultimate responsibility for the product security, and a separate product development team with no cyber-security expertise. This approach has led to the lack of ownership of security from the product team. In this case, the security team mandates the implementation of the Software Security Development Standards, but doesn't yet have the necessary clout to enforce them. The product team, on the other hand, is under tremendous pressure to release competitive products, and frequently by-passes necessary security checks and balances, creating additional risks.
3. The third approach is the combined internal responsibility for the product design and security, "under one roof". In this case, all company officers and product developers come from the banking sector where security and risk have been a part of the core business since inception. In this case, security is always a part of the discussion, with

every release. In fact, it is acknowledged to be one of the main "pain points", causing as much as 80% - 90% of the releases to be delayed or reduced in scope. Still, at the end of the day, the team has strong confidence concerning the security of the released product.

As can be seen from the above examples, despite having equal pressure to release the product, those companies where security was considered to be one of the core features of the product and "owned" by the product design team, had a far better processes to reduce risk. Interestingly, negative impact on the product features and time to market was much greater at those firms with greater awareness and full ownership of the security risks.

Strategic technology-enabled innovations focused internal processes

This category of technology-enabled innovations are not customer facing, but are still strategic in nature. For example, a supply chain automation project that is set to significantly lower costs may be a part of the overall cost reduction strategy set by the CEO of the company. Other projects include things like improved productivity, better customer relationship management, employee relationship management and many others. The key to recognize these projects as strategic is their direct association with the company strategy.

A number of interview companies maintained strategic technology-enabled innovations agendas, fully supported and monitored by the board of directors and the executive leadership teams. The same companies also explained that their boards were aware of the increased risk of cyber-security, and therefore, seemed to have a rather balanced approach to managing added risk.

Since the innovations were not associated with direct product release, there seemed to be a lot less pressure applied on the innovation efforts, giving more room to the various governance and monitoring practices. Interestingly, most companies have experienced recent increased interest and an increased number of technology-enabled innovation initiatives, creating growing queues of projects and increasing the computing environment.

The centralized and strategic nature of these initiatives tended to be associated with the most well managed, well understood security practices. Here are some examples of the described projects in this category:

- Mobile apps for employees;
- Move to the hybrid cloud to reduce data center costs;

- Move to the Office 365 cloud;
- Improvement in network resiliency and "uptime".

Tactical technology-enabled innovations at the operating unit level

This category of technology-enabled innovations are associated with a wide variety of technology-enabled innovations that are being planned and executed at the operating unit or a department level, without having a direct link to the company strategy. They tend to have lower budget, shorter timelines and benefit only that specific operating unit or department.

This approach to technology-enabled innovation presented another set of challenges. It was most apparent in companies that have grown through merger and acquisition activities or were organized into large groups of regionally distributed offices with a lot of autonomy and decision making power. In these cases, culture, regulatory environment and organizational awareness played a critical role in determining whether cyber-security efforts were effective, and how or whether they were properly applied to various innovation activities.

Effectively, when innovations are taking place at the operating unit level, the key is to ensure that each of the proposed technological changes goes through a security review. This requires a number of factors to be in place:

- The organizational unit needs to be aware of the importance of this step, and not be inclined to skip it in favor of faster implementation;
- A stronger measure would be to ensure that the organizational unit has a strong incentive not to skip any steps in security evaluation, for example, steep financial penalties for non-compliance with PCI standards on the annual review;
- Assuming that the organizational unit is aware of the need to review all of their new technology initiatives for cyber-risk, they need to have access to these services, either through in-house expertise, a corporate security team or through an authorized third party security services firm.

These steps are not easy to follow, and even harder to monitor. Therefore, frequent reviews, monitoring, measurements and a strong incentive system (internally or externally imposed) is highly recommended for companies innovating with technologies at the business unit level.

Publicity of cyber breaches

The nature of publicity of cyber-breaches

It appears that another strong driver of the cyber-security efforts inside a firm is the history of breaches in their industry, and related publicity. In fact, there are very specific impacts that I would like to list.

- Certain industries have had multiple widely publicized breaches, so much so that not only executives, but also the middle management and front line employees have become aware of the risks;
- In some industries, breaches have resulted in severe negative business impact and dismissal of Chief Executives. Firms in these industries have demonstrated strong board level support and frequent intense discussions with the board;
- In the industries where only one or two incidents have occurred, there is still not enough appreciation for the risks. Although boards are interested and appear supportive, the big push-back comes from the middle managers who generally don't draw parallels to their own operation, and feel the risks are simply too hypothetical;
- Companies in the industries where no publicized incidents have occurred tend to have a harder time creating the awareness.

Additionally, there are various types of breaches and related publicity. The biggest publicity comes from larger breaches, such as Sony, Home Depot or Target, or in cases where hackers ensure that the breach is made public.

Some of the hacks that don't get widespread publicity still get circulated within the industries themselves. For example, the news of the Ukraine's Prykarpattyaoblenergo utility as the first known power outage caused by a cyber-attack, has quickly spread throughout the world among the energy management companies. It is not clear, however, that this single incident would be enough to generate the necessary level of awareness and drive the required attention to the cyber-security efforts within those companies.

Verizon's 2015 Data Breach report categorized "successful" breaches by size and by industry.

Table 13 – Security incidents by victim industry and organization size

	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31–33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44–45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48–49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

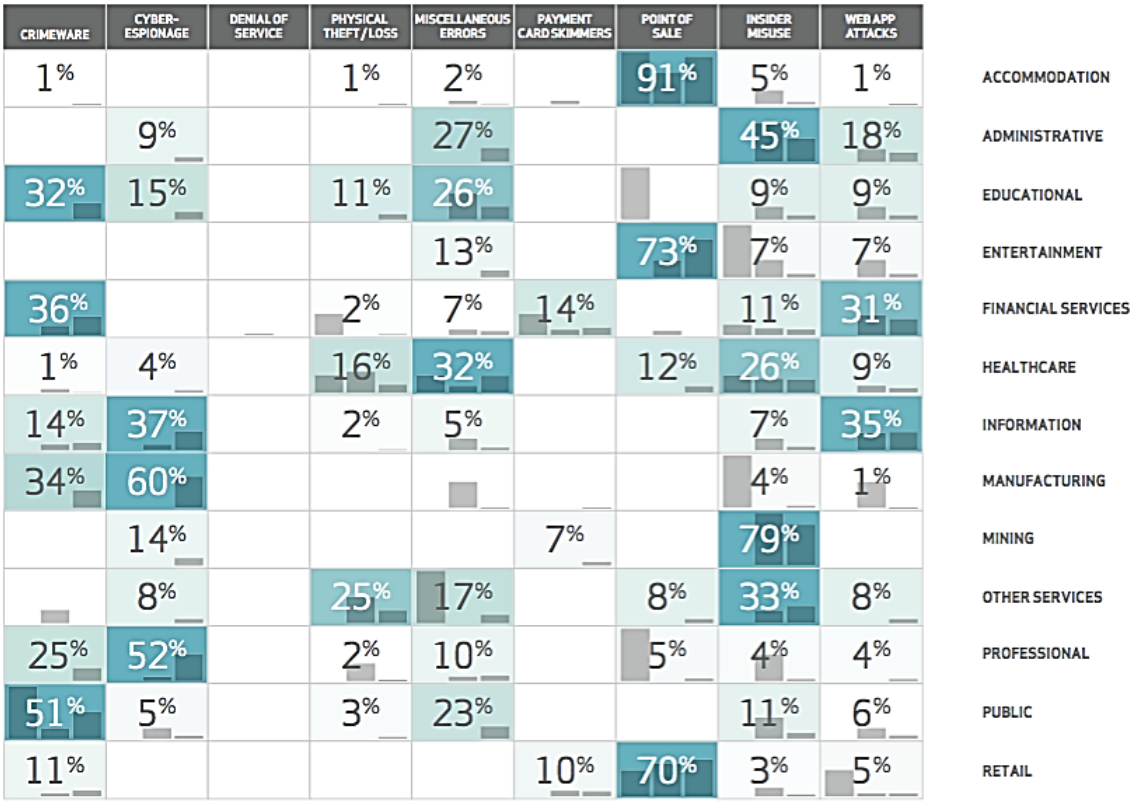
Source – Verizon 2015 Data Breach Report

One notable point about this report is the focus on data breaches, as opposed to overall cyber-security breaches. For example, this report would not capture an attack of control systems such as that of the Ukrainian power plant in December of 2016, when hackers took control of the system causing thousands of people to loose electicity to their homes. In this case, no data was lost but instead control of a critical infrastructure was taken over.

This power plant example shows the breadth of the cyber-security field. However, the table is still a helpful gauge of the industry specific impacts.

The same report also provided the information around the disclosures of the breaches by industry, as well as the type of attack. This table will help companies better understand industry level exposure, by the size of the company, and enable then to compare to their own results. For example, within the private sector, financial services, retail and manufacturing seem to have the highest number of incidents and confirmed losses, while transportation and utilities so far have had much lower number of incidents.

Table 14 – Frequency of data disclosures by incident patterns and victim industry



Source – Verizon 2015 Data Breach Report

Of these sectors, the most publicized incidents applied to the following groups:

- Accommodation (various hotel companies);
- Entertainment (Sony);
- Financial Services (JP Morgan);
- Healthcare (Anthem insurance);
- Information (Ashley Madison);
- Public Sector (OPM Government data breach);
- Retail (Target, Home Depot).

Finally, in every industry there seems to be a particular event that tends to be the inflection point to spur interest, attention, board interest and budget allocation for the cyber-security teams.

Examples

One of the European based interviewees shared an interesting story: very recently, one of the European based telecommunications providers experienced a very large, widely publicized data security breach. In the process of managing the crisis, the CEO appeared before the press and gave some information to the reporters. The CEO's interaction with the press, when observed by her peer in the interviewed firm, gave them such a scare that in addition to the existing and fairly mature cyber-security processes and efforts, the company has opted to create another cyber-security review project, doubling down on the efforts and the budget. It is not sure whether this new effort would be helpful, but certainly, when the CEO has a strong incentive to avoid cyber-security related incidents, there is a strong impact on the rest of the organization and the cyber-security team in particular.

Chapter 5: Impact of various organizational dimensions

I will now examine a number of firm-level factors that impact the balance between innovation and cyber-security.

Operating Model and Organizational Structure

One of the strongest factors impacting both cyber-security and the innovation efforts in the organization appears to be the operating model and the organizational structure.

Various types of organizational models and their impact

The first example is the diversity of the business. Companies that operate in various businesses (i.e. conglomerates), require a wide variety of cyber-security personnel specializing in various industries where the firm operates, and covering different types of technologies. Additionally, different companies under the umbrella are regulated by different entities and therefore, require different reporting and compliance mechanisms. Finally, technologies and vector attacks vary widely, and need to be understood and managed on a per-segment level. The same issues apply to the innovation efforts: each business under the group umbrella competes against others in their industry, and therefore, requires industry-specific innovation in technologies. The only company wide centrally managed technologies in this case are the fundamentals, such as desktop, communications and office productivity tools.

The second example of the challenging operating model is the geographical diversity, especially international diversity. These companies now have to closely follow and comply with country specific legislation.

The last, and perhaps most challenging example of the operating model implication, is the example where various business units have separate P&Ls and a lot of autonomy in the decision making process. This is frequently combined with the geographical diversity, adding to the complexity of the issues. One of the interviewees described this environment as follows:

> "Imagine that you are standing in the middle of the Grand Central Terminal, trying to keep track of all departing trains, and ensure that they all have been checked prior to departure".

This scenario was repeated across several of the interviews, but they all have had a common theme: it all came down to education and measurement. Those business units where leaders were fully educated about the cyber-risk and took it seriously would fully support all

cyber-security standards and initiatives; conversely, problems with compliance would usually originate from the branches or business units where cyber-security was not considered a high priority. When combined with the tactical innovation mode and lack of measurement, those business units' security issues could potentially go unnoticed. Interestingly, several such firms introduced unit-specific compliance reporting tools that were periodically reviewed by senior management, and such reports provided an excellent mechanism to generate remediation activities. Additionally, these firms have sited frequent and on-going "re-education" efforts, to address the management turn-over in the business units.

By contrast, companies with a centralized business model had a much easier time in ensuring that cyber-security processes and practices were fully incorporated into all technology-enabled innovations activities, as well as all "business as usual" management activities.

Another interesting dimension to examine is the reporting structure of the cyber-security team itself. A few options have been observed with the interviewees:

- Outsourced to a trusted cyber-security partner;
- Product cyber-security team is completely separate from the enterprise cyber-security team;
- Cyber-security team is part of the IT group;
- Cyber-security team is outside the IT group, and reports to other entities.

To further drill down into the detail, here is a summary from the survey data.

Table 15 – Cyber Security Reporting structure

9. Cyber-security Reporting structure. Please identify who cyber-security unit reports to within your organization.

#	Answer	Response	%
1	Board of Directors	8	13%
2	CEO	9	15%
3	CFO	3	5%
4	CIO	30	48%
5	Legal	2	3%
6	Other	10	16%
	Total	62	100%

Other
Dual reporting to head of IT and Board
Chief Corporate Security Officer
Everyone
Planning
Director of Enterprise Technologies
Na
Each division
Director of IT

One of the interviewees used to report to IT, but recently has transferred to report to the Chief Corporate Security Officer, which included Legal, Risk and Compliance responsibilities. In the interview, this was perceived as a very positive move, giving this security officer a much stronger mandate and much higher level of authority. However, extra efforts will be required to stay current and collaborate with the IT team in following all of the developments and the innovations. This interviewee was also regulated by PCI compliance standards, which requires frequent reviews of the perimeter and the changes in the computing environment. Therefore, combining the separated reporting with the strict and on-going compliance environment seems to be a very beneficial and practical move.

However, there is another interesting trend that emerged in the interviews: several large companies with strong governance and risk management cultures have found themselves to be too slow and too bureaucratic to respond to the competitive pressures in terms of technological innovations. To compensate for this, they funded start-ups or bought existing start-ups that operated in the lean and agile mode, and created innovative products with much greater speed. Since these start-ups were set up as their own entities with little or no governance or oversight, cyber-security maturity of the products were directly dependent on the expertise of their software developers, and the awareness of the start-up executives.

One of the interviewees offered an excellent solution employed in their decentralized company: in addition to the Enterprise IT group, there is a cyber-security outreach group that is the point of contact between the Digital Risk and Security team on the one hand, and the Operation units on the other. Their role is largely educational; they are largely cyber security "missionaries". This is working extremely well in Europe, and is currently being promoted in other parts of the world as the best practice.

Summary of the insights

- Companies with a decentralized operating model are at a disadvantage in terms of cyber-security management. This is especially so if technological innovations happen at the unit level, as opposed to a centralized effort;
- Best practice in monitoring cyber-security of diversified technology innovation efforts is to manage and monitor the implementation of cyber-security standards, combined with frequent reviews and executive level reporting;
- Cyber-security reporting outside of IT can be effective and add the needed level of authority to the team, provided that they are supported by strong levels of monitoring, senior management support and frequent and transparent reporting mechanisms;
- Outsourcing of the product development to start-ups is a common trend. The parent companies must ensure that the funded start-ups have the right expertise and appropriate levels of incentives to ensure that the needed security is built into the product;
- Cyber-outreach teams that bridge the gap between Enterprise Security and various operational business units is one of the best practices that seems to be working well to close the security gaps and enable secure innovations.

Company culture and tensions created by cyber-security efforts

Why culture has an impact on the balance between innovation and cyber-security

Based on the unanimous opinions of interviewees, company culture has strong impact on a firm's management of cyber risks. This comes from a variety of factors.

The first factor is rooted in the historical understanding of risks: firms that operate in the financial sector have not had a lot of challenges in creating the necessary organizational awareness, because appreciation of the risk management efforts seems to be in the DNA of the finance professionals. This became evident in the interviews with the financial services companies.

In contrast, the most painful experience raising the awareness of cyber-security efforts seem to come from the engineering based culture. In fact, every interviewee that operated in an engineering based culture shared frustration around their ability to convince the operators to see the associated risks, and change their processes. The same interviewees acknowledged the increased levels of pressure to innovate using technologies, both in terms of the product features and also in the manufacturing process.

In one case, company culture was so strongly driven by the timely delivery of the new product lines that "if the product release gets delayed, people responsible would lose their jobs". This culture, when combined with weak incentives and lack of cyber-security regulation, creates new levels of risk taking culture and a set of unintended consequences that will play out in the future. At the same time, these newly created risks don't seem to be fully understood and are not measured. These new and unmeasured risks are effectively the "price to pay" for the timely and on-plan product releases.

By contrast, financial services technology innovation products described by one of the interviewees all go through rigorous security review, and as much as 80% - 90% of them go back for "security tune-up", causing both delays and in some cases changes in feature functionality. Delays and scope changes, in this case, are the "price to pay" for the reduced and well understood risk in the product.

The tensions between the IT cyber-security teams and the local operations teams seem to be more pronounced in the operations driven engineering cultures combined with an organizational structure where local operations teams have the decision making authority. Going back to the example in the prior chapter, a cyber security outreach group is an excellent

solution to help resolve conflicts an ease tensions between the IT and the local operations teams, but it does require extra funding and resources.

Example

One of the manufacturing firms was planning to release an in-home product that had cloud connectivity and an associated mobile app. Due to project time constraints, the project team chose to skip the required penetration testing steps and went ahead with its release. The security had to be addressed in the later releases of the product.

Summary of the insights

- Company culture can play a positive or a negative role in establishing mature cyber-security efforts. It appears to be linked to the prior experience in risk management from company operators and executives;
- There is a clear trade-off between innovation and cyber-security in companies with technology-based product innovations: "risk aware" cultures tend to delay product releases or reduce product features, viewing it as a "price to pay" for well understood and calculated risks, while "risk unaware" cultures tend to favor timely product releases with maximum feature sets, at the expense of unknown risk creation.

Board of Directors and their role in cyber-security and innovation trade-offs

How board of directors engage in the cyber-security risk discussions

A majority of the interviews and surveys confirmed that in the recent years there has been a strong level of interest and participation of the boards in cyber-security oversight. As previously discussed, negative industry related publicity that "hits close to home" seems to further strengthen board level engagement with the cyber-security team's efforts. Board briefings range from quarterly to annual updates (Figure 23), with quarterly reviews being most common among respondents. Most commonly, these meetings are being described as interactive (Figure 25), and last between 30 minutes to one hour (Figure 24). To further confirm these findings, the tables below represent summarized findings on the frequency, the length and interactivity of the board meetings.

Figure 24 – Frequency of cyber-security briefings to board of directors

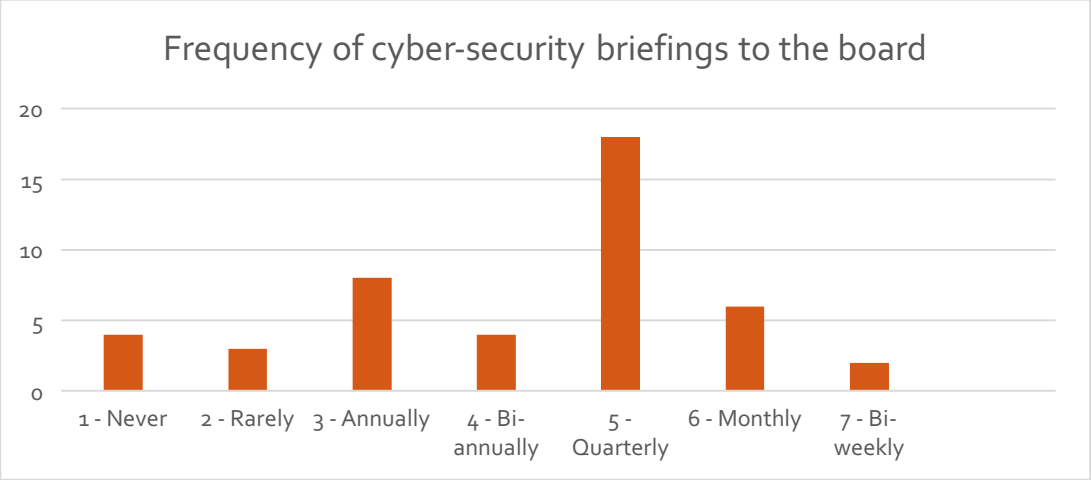


Figure 25 – Length of the board briefings on cyber-security

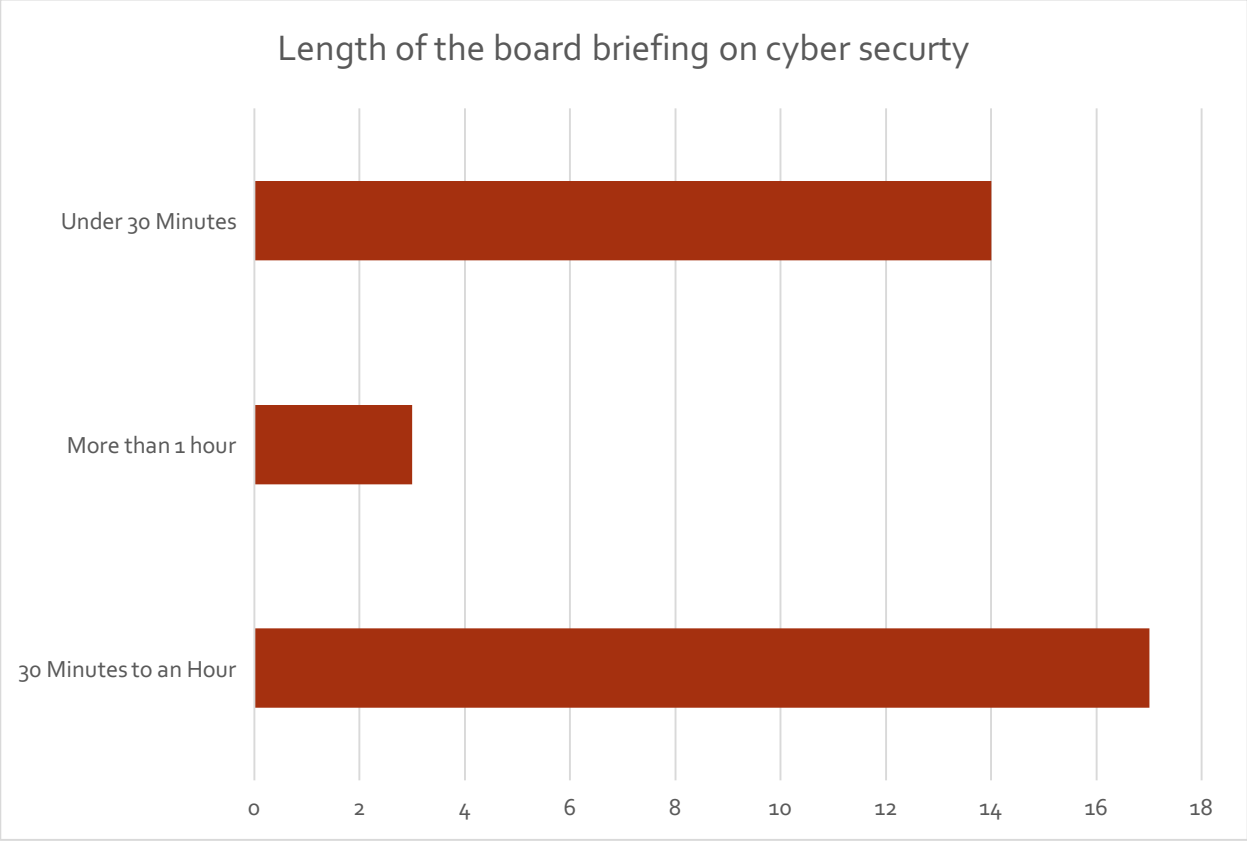
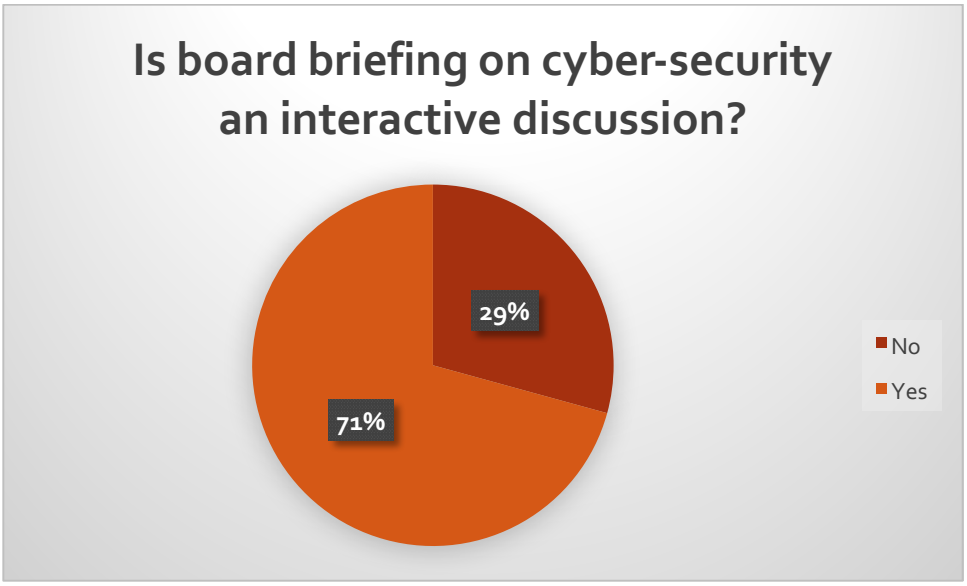


Figure 26 – Interactivity of the cyber-security briefings to the board



In most cases, the board supports and approves funding for all initiatives supported by the cyber-security team, and in no instances has the board been identified as the "bottleneck" in the process.

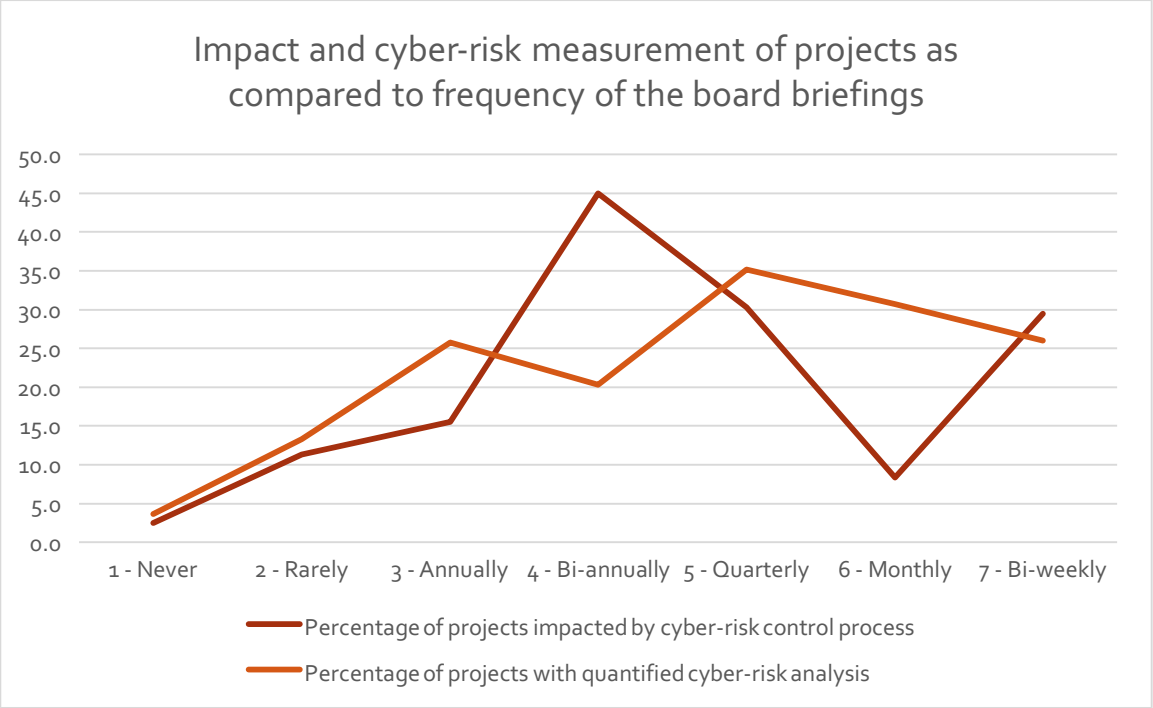
In some cases, boards have taken additional steps to further increase the effectiveness of the cyber-security team:

- In several cases, boards required the IT Security team to create and regularly update a set of quarterly KPIs, allowing them to create transparency into the efforts and help monitor the progress;
- In one instance, following a particularly negative and publicized security breach in the region, board created an additional committee to help elevate cyber-security efforts and ensure that maximum efforts are being applied by the company.
-

Finally, in trying to establish best practices that on the one hand reduce negative impact of the cyber-security controls on the innovation agenda, while on the other minimize the risk and strengthen the security posture of the firm, frequency and interactivity metrics were compared with the impact on technology-enabled innovation projects.

The Figure 27 below compares the impact and cyber-risk measurement of projects as to the frequency of the board briefings.

Figure 27 – Comparison of the impact and cyber-security measurement to frequency of the board meetings

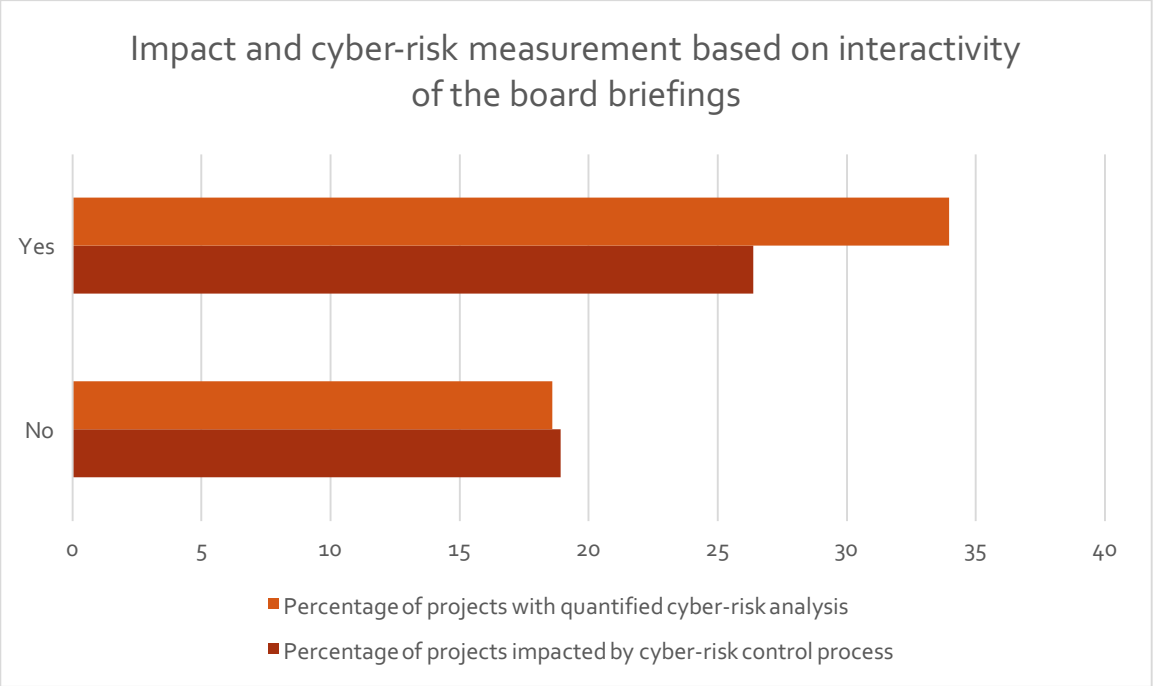


Here are a few analysis points based on these findings:

- More frequent cyber-security board briefings are generally associated with higher levels of cyber-risk measurement as well as higher impact on the technology-enabled innovation projects;
- Quarterly cyber-security briefings, which are also most common and where we have most data, show 35% of projects having cyber-risk measurement and 30% of projects being impacted by cyber-security controls;
- Other data points are not being analyzed due to a small data set that may lead to the wrong conclusions.

To understand the impact of interactivity of the discussions, the following compares that data point against the impact of cyber-security controls and cyber-risk measurement.

Figure 28 – Impact and cyber-risk measurement based on interactivity of the board meetings



From this chart, we can clearly see that interactive discussion about cyber-security and cyber-threats at the board level leads to a significant increase both in terms of the impact on the technology projects and the degree of cyber-risk measurement. This is a natural and expected result, as people that talk through issues are likely to take a more active role in the governance of the cyber-risk.

Misaligned incentives at the middle management

Although strong support from the board is absolutely necessary and fundamental, it is definitely not sufficient. Based on some of the interviews, despite strong support from the board and sufficient funding levels, company middle management and lack of awareness continued to block the efforts of the cyber-security teams. Many times, when reading articles or speaking with business leaders about this issue, it is discussed in the framework of "IT Leaders (CIO/CISO") and "Board/CEO". Although it is true that perhaps those leaders are the ultimate decision makers and drivers of change when it comes to security, they are the only people that potentially have the strong incentives to get security right. In almost all of the interviews, boards and the CEO were very interested to get their cyber-security right, and have been willing to provide resources and funding. Additionally, in almost all of the interviews IT

executives were highly motivated to do the right thing, however, were frequently held back from doing so elsewhere in the organization.

In many companies innovation efforts are managed outside of the IT organization while the cyber-security efforts are the responsibility of IT. In these situations while boards and the CEO are informed of both innovation and cyber security activities they frequently do not have the transparency into the trade-offs between product releases and cyber-risks. Only when the incentives on these efforts are tightly aligned and trade-offs are transparently discussed, can the CEO and the board get the visibility and make the appropriate adjustments. This is probably the biggest "blind spot" in the technology-enabled innovations efforts identified in these interviews.

Deeper examination of the board member responses to the survey reflects the fact that in some companies, some of the boards are still in the "discovery" mode as opposed to the "governance" mode when it comes to cyber-risk, and clearly this process needs to evolve, allowing for more mature reporting and higher levels of transparency including the risk/rewards trade-offs in the technology-enabled innovation efforts.

Summary of the insights

- All boards are concerned about cyber-security, and most are actively engaged in the discussions;
- Many boards are still being educated as opposed to playing a strong governance role in cyber-security;
- Many boards are not aware of the trade-offs that are being made between technology-enabled innovations and cyber-risks, and therefore are not in the position to provide oversight over this "blind spot";
- Boards that have insisted on having regular cyber-security related KPIs and dashboards, especially if they are done at the business unit level, have been most successful in driving organizational culture;
- Boards appear to be most sensitive to the industry specific and regional publicity of cyber breaches and tend to step up their efforts following such events;
- Best practice of the board briefings on cyber-security is to have interactive quarterly updates.

Education, communication and organizational awareness

How companies create awareness of cyber-security risks and best practices

Education, communication and organizational awareness clearly has a strong impact on the effectiveness of the cyber-security efforts. However, the effectiveness of the educational efforts appears to be predicated on a number of factors, and is further amplified when multiples of these factors are applied at the same time:

- Support from the board of directors;
- Presence of business unit measurements and accountability;
- Prior and recent history of publicity around security breaches in the industry or in the region;
- Company culture, and prior experience with various risk management activities.

For the educational efforts to be fully effective, they must be incorporated into the on-boarding processes and occur regularly. Some of the respondents rely on videos and webinars as methods of delivering educational material. By far, the most effective educational approach described has been that of the cyber-security outreach group, which is effectively a dedicated cyber-risk education and awareness entity embedded into the operations of the company.

When it comes to the innovation efforts, general organization awareness is not nearly sufficient, and additional education is required, specifically:

- Managers responsible for product development need to be educated and fully aware of the cyber-risks, so that they can be in the position to fully understand these risks, and be able to discuss the trade-offs between new product features and corresponding risks. This appeared to be a "missing piece" in a number of interviews;
- Engineers responsible for product creation must be fully trained in the best practices and be completely aligned and empowered to follow the Software Security Development Lifecycle process and standards established by the company, including all required testing, review and remediation requirements. In some interviews, although engineers were trained, they were not supported by the product managers in these efforts;
- Software engineers need to be regularly certified and re-certified in the secure application development methods and practices; it was not clear whether this was done consistently;
- Cyber-security team must continuously receive education in all new threats and emerging trends in the cyber-security practices; most teams appeared to be actively engaged with their peers and seemed to attend all of the conferences and be up to speed on the tools.

Summary of the insights

- Education and awareness are critical to the success of the cyber-security teams, and a number of best practices exist to manage this effectively;
- Education and awareness can be effective only if other best practices of cyber-security processes are being followed, namely senior management commitment, measurement and accountability;
- Teams responsible for innovation efforts require additional levels of on-going training, including product managers; some teams seem to be lacking this specific level of awareness.

Chapter 6: Technology and IT Management practices

As one might expect, technology management practices seem to play an important role in a company's ability to innovate securely.

Standardization and legacy architectures

Why standardization and updates matter to both innovation and cyber-security

The first and perhaps the most obvious enabler of the technology innovation effort is associated with the standardization of the existing systems. Simply put, those companies that have standardized on their technologies across business units are in a much better position to enable and scale their innovation efforts. Standardization also allows companies to have a much better handle on securing these technologies. Therefore, companies with standardized technology platforms have, in essence, "the best of both worlds" and are much better positioned for the future.

The second related point is the legacy architecture. In some companies, centralized or not, a number of deployed applications are still "legacy", which creates additional challenges in securing them. This is particularly challenging when these legacy applications are deployed in a decentralized environment.

Examples

One of the vivid examples comes from a company where a number of legacy applications had hard-coded default passwords, some of which were even published in user manuals. At one point, one of the hacking organizations publicized a list of these hard coded passwords, immediately exposing the company and all other companies using these technologies. This event forced the company to work with the manufacturer and close the security gaps. However, several other similar implementations are still in place and without a complete re-build, securing them becomes a very difficult task.

IT Governance and resource allocation

Why governance is important to achieving the balance of innovation and cyber-security

Another set of challenges that impact both the innovation and security agenda comes from the maturity of the IT Governance function. Some of the respondents have strongly governed IT organizations. When such culture exists, IT Security principles seem to be strongly observed and supported by other IT functions, namely:

- Well governed IT shops have a strong understanding of their assets and inventory, allowing for better monitoring of the environment;
- A couple of interviewees demonstrated a clear, strategic approach to addressing their cyber-security posture;
- They tend to have better resilience, as well as documented disaster recovery and response plans, mitigating the risks in case of a breach;
- Well governed software development teams tend to follow security architecture and review processes at every step, starting from the design phase, and tend to be in better shape with the final product;
- Well governed IT organizations have well-established communication protocols with senior management, and therefore can cover both value creation and risk management discussions at the executive leadership meetings and at the board level;
- Finally, well managed IT environments tend to attract and retain stronger talent and work with more competent and fully accountable trusted partners, both in their innovation efforts and cyber-security efforts.

Resource allocation

Another big component of IT Governance is the resource allocation discipline that applies both funding and talent.

In terms of funding, several respondents have raised it as an issue, and particularly pointed out that cyber-security budgets are "competing" with other initiatives many of which are allocated to the innovation projects. This, in fact, has been my personal experience as well.

To resolve this, companies should establish and utilize strong technology investment principles and formalize an "IT demand management and prioritization methodology", which is one of the IT governance best practices that would help make these decisions more transparent and resolve some of the tensions.

One of the respondents in a highly regulated industry is required to present the case for each line item in the budget on its own merit to a series of committees who then decide which projects go forward. In his case, cost efficiency tends to be the driver behind most decisions, and therefore, all projects are looked at through that lens. This includes the innovation and the cyber-security projects. With this style of governance, having truly innovative projects approved is equally as hard as having cyber-security projects approved.

By contrast, in my previous job, our formalized demand management IT projects approval methodology was set up in such way that mandatory projects took priority, since the environment was regulated by PCI. Therefore, cyber-security projects always received funding and talent, while various innovative projects had less chance of going ahead.

Example

In one most extreme case, a marketing company offered their services though a technology platform. As part of the platform functionality, customers' credit cards were being recorded and stored on behalf of the firms' customers. Several years ago, customers started asking whether the platform was PCI compliant, and eventually, started to demand it. Furthermore, signing up new customers also became predicated on having the platform being PCI compliant and on maintaining this compliance on an annual basis. The company's CEO and the board recognized this as a priority, and prioritized PCI compliance as the main and only project in terms of the platform advancement. All other projects had to be put on hold for a year. Achieving PCI compliance was a very expensive and difficult project. The cost of the project itself in combination with the economic cost of not moving ahead with any other advancements demanded by customers was quite significant. This experience demonstrated to the management team that "bolting" security on at a later date is extremely costly and inefficient, as compared to addressing security up front and building it into the design, development and execution steps of the process. This lesson in economics has led to the creation of the new Software Development Lifecycle Standards (SDLC), much greater awareness of the trade-offs in the executive team and much better awareness and education of the development team. A year after this event, a CISO received a call from one of the software developers, apologizing for missing one step in following a specific security-related step in SDLC, and wanting to rectify the situation as quickly as possible. This example demonstrates a noticeable change in the attitude among the software developers: they knew that cyber-security was important, they knew that all of their work would go for review, and

were comfortable to follow the newly established SDLC process. In all of the interviews conducted, this was the best example of well-governed cyber-security risk in the development environment.

One of the other examples of good governance comes from a European bank that chose to launch their mobile banking app on iOS, holding back on the Android release for more than two years to protect their customers from a series of security challenges and taking their time to close all known security gaps.

An example of an evolving security governance culture comes from a company that has done an outstanding job in creating thorough, well documented standards and best practices covering both the traditional waterfall as well as the newer agile software development processes. The same cyber-security group is still working to establish the necessary corresponding monitoring and reporting tools, and is operating in a strong operations centric engineering culture with immense pressures to innovate on the product with the new technology-enabled features. With these pressures in place, existing standards are only a piece of the puzzle, and many other steps must be taken to achieve the desired level of maturity in their cyber-security measures.

Another example comes from the interview with head of innovation at a retail healthcare and pharmacy company, regulated both by HIPPA and PCI. A few years ago the firm had to deal with a breach and learned about the impact to their business. To find new sources of growth the company has set up a separate innovation unit. This highly competitive innovation unit constantly experiments with a wide variety of products and services. In the experimentation phase, they try to rely on existing technologies, and focus only on finding the answer to the question: does this idea have a merit? However, to implement these ideas into reality, in nearly 100% of the cases they require their IT department to enable these innovations. Therefore, if an idea is deemed to have merit, the IT department and the risk-management team (in this case, the Legal department) are brought in to evaluate the risks, the costs and the resource requirements, including time, funding and people. To quote the interviewee, "risk reward discussions do happen all the time. It's an active discussion. Tensions are created between Legal, IT, and Innovation teams." However, when asked about the negative impact, the head of innovation struggled to understand the question. Upon further discussion, it became clear that delays and scope changes are understood as necessary, unavoidable aspects of various technology-enabled innovation projects. Furthermore, projected project timelines and budgets have a certain amount of risk and unexpected delays built-in and therefore, are not really perceived as negative impacts but rather as fundamental necessities of such projects.

Summary of the insights

- Well-governed IT groups are better prepared to address technology innovation and cyber-security needs of the organization, regardless of the insourcing / outsourcing model;
- Governance efforts are especially effective when combined with transparency, reporting, supporting culture and organizational awareness;
- The total economic cost of adding security after the fact is significantly higher than building it in from the start;
- Budget and resource allocation should always include a certain amount of delays and scope changes.

Chapter 7: Innovative technologies and related cyber-security implications

Many big trends are responsible for rapid changes in the economy: cloud, big data, mobile, social, IoT, 3D printing, robotics, blockchain and others. These trends serve as a proxy for the impact of technology maturity on technology-enabled innovations and their trade-offs with cyber-security. I will examine a select number of these trends, to contrast potential value creation of these technologies with the corresponding cyber risk and potential value loss. I will then examine the data from the survey responses and the interviews, to provide additional insights and evaluate patterns in how various companies are dealing with the technology-enabled innovation and cyber-security trade-offs.

Example of mature technologies: Payment Technologies

I would like to start my analysis of the latest technology-based innovation trends by examining the latest evolution of the payment industry and related technology. I take this approach for a number of reasons. First, I was personally involved with customer data and payment technologies for many years, starting with the data privacy issues, and then living through many iterations of these technologies across various retail channels, as well as managing the security and the compliance issues, so it is a subject I know well. The second reason I would like to start there is because it is one of the areas that perhaps has been affected the most and has evolved the most, in terms of addressing the cyber-security concerns.

Evolution of payment technologies and related cyber threats

Electronic payments trace back to the 70s, when Electronic Data Exchange (EDI) was introduced, later to become the basis for electronic transactions. In the 80s and the 90s, with the introductions of modems, credit card transactions became automated, and a few years later, faster internet-based connections and security protocols were established to speed up these transactions.

In the 90s and 2000s, many companies set up their on-line shopping portals. However, it was not until transactions could be completed "end to end", including payments, that e-commerce business really took off. Today, we are at the point where e-commerce retail

numbers are starting to surpass those of "brick-and-mortar", especially in more technologically advanced countries such as China and Norway.

With the proliferation and maturity of smart phones across the globe, another revolution in payment technology started to take shape. In the last few years, a famous Starbucks Mobile Payment app has gained great popularity, and continues to be one of the most innovative platforms. Apple Pay was launched in 2014, and Samsung Pay in 2015. Walmart is ready to launch their mobile payment app in 2016. Alibaba and Tencent in China have long been using mobile payments, and Alibaba has plans to launch their payment business in the US. Facebook and other social media platforms are also planning to enter this space. Of course, the incumbents, such as banks, credit card brands and payment processors are all launching their mobile wallets. Even the telecommunication companies in various countries are planning to launch payment products. Finally, as bitcoin and other digital currencies starting to mature, there is another potentially highly disruptive payment technology that might once again change the landscape.

The reason such a high level of activity is taking place is simple: everyone recognizes new market opportunities offered by mobile payments, and is trying to move in quickly and leverage their market power to take a share of that market. Such levels of competiveness require enormous levels of innovation, and companies are racing to ensure they have a firm hold. So, although the electronic payments have been around for a long time, they are in fact one of the most advanced and more disrupted innovation technological areas of our time.

Unfortunately, these advancements in payment technologies continue to attract high numbers of fraudulent activities. In the early 2000s, credit card fraud was a significant problem for the credit card companies and was eating into their profits. To combat this new form of fraud, credit card companies (Visa, American Express, Discover, JCB and MasterCard) formed a Payment Card Industry Security Standards Council and created the industry's first Payment Card Industry Standard.

At first, these standards focused on the processes, the standards and the governance issues. Since credit card payments continued to be a mix of physical and electronic activities, the PCI standard addressed both of those "worlds". Since I was involved with PCI compliance activities from their inception, I would like to use my personal experience to briefly describe its evolution from the IT management perspective.

At first, PCI compliance didn't have any "teeth" associated with it, and was just a matter of best practices and paperwork formality. At that time, most companies went to their Point of Sale software vendors and insisted on getting the latest PCI compliant and certified

software versions. This was an important first step. However, in 2007 a very large credit card breach at TJ Maxx became widely publicized, and gave additional credence to the PCI program. Many well governed companies took it upon themselves to step up their efforts. Additionally, many IT security consultants quickly got up to speed on PCI standards and obtained necessary certifications, generating strong growth in the IT Security industry.

Meanwhile, the PCI council continued to be hard at work, investigating new threats and periodically releasing the new versions of the standard. Each new version closed the known gaps, not only in terms of the processes and the governance, but also in terms of addressing new technologies that emerged since the previous standard, new tools such as monitoring, and even new commercial requirements. For example, PCI 2.0 provided a lot more specifics related to the Wi-Fi enabled payment transactions. What perhaps is even more interesting is that PCI 3.0 started to address the supply chain issues: it is no longer acceptable just to contractually require your providers to be PCI compliant. The new PCI 3.0 standard requires high-volume Level 1 merchants to do periodic site inspections by authorized and certified personnel to ensure that their providers are in fact in compliance. Finally, in the last few years PCI and the banking industry have gained very strong power and started to impose serious financial penalties on non-compliant merchants. It also introduced a "liability shift" concept and a deadline in various countries, which meant that as of that date, non-compliant merchants would carry a financial burden of all costs related to the breaches associated with transactions at their facilities. The standard equally applied to all retailing channels accepting payments: in-store, on-line and over-the-phone. Some companies even had to stop accepting credit card payments in certain channels until the compliance matters were fully addressed.

Even with this level of rigor and strong financial incentives, we continue to read about credit card breaches in well-known companies. This is because, as described in the Verizon's 2015 PCI Compliance report, cyber criminals shift their focus from more secure to less secure transactions, constantly looking for more "cost effective" ways of stealing. Verizon uses Canada as an example of this phenomenon: when Canadian merchants went to "chip and pin" enabled technologies in the 2008 – 2011 timeframe, the fraud gradually "migrated" to "card not present" transactions, such as on-line payments and call center payments. This can easily be seen in this graph:

Figure 29 – Payment card fraud losses

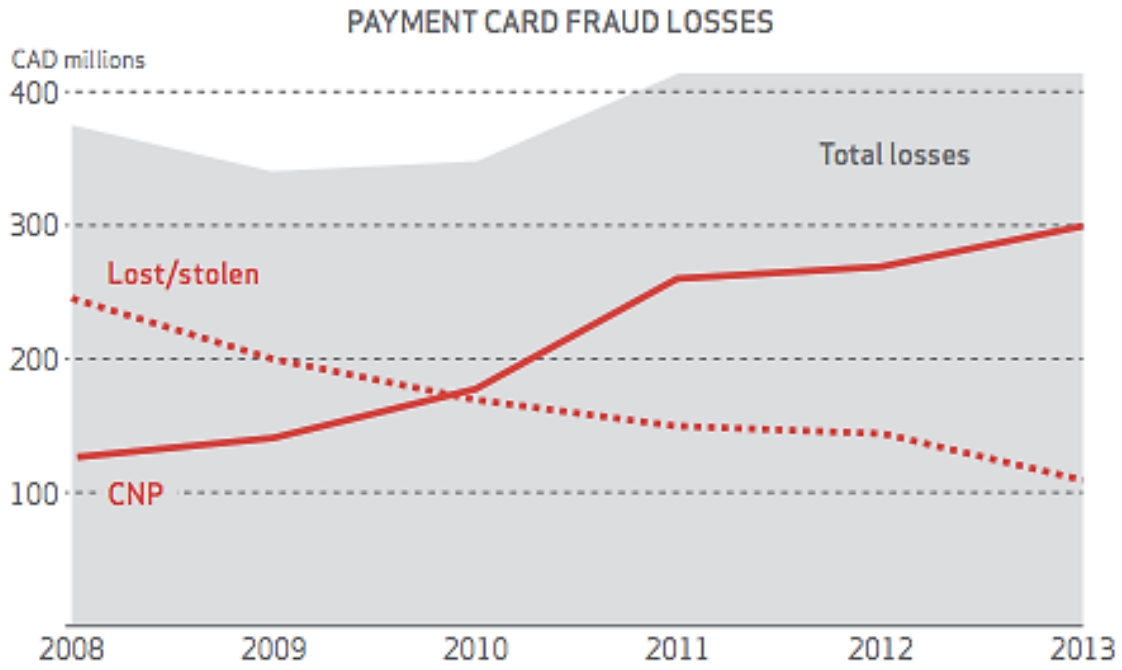


Figure 7: Card fraud in Canada, 2008–2013 (data from Canadian Bankers Association[7])

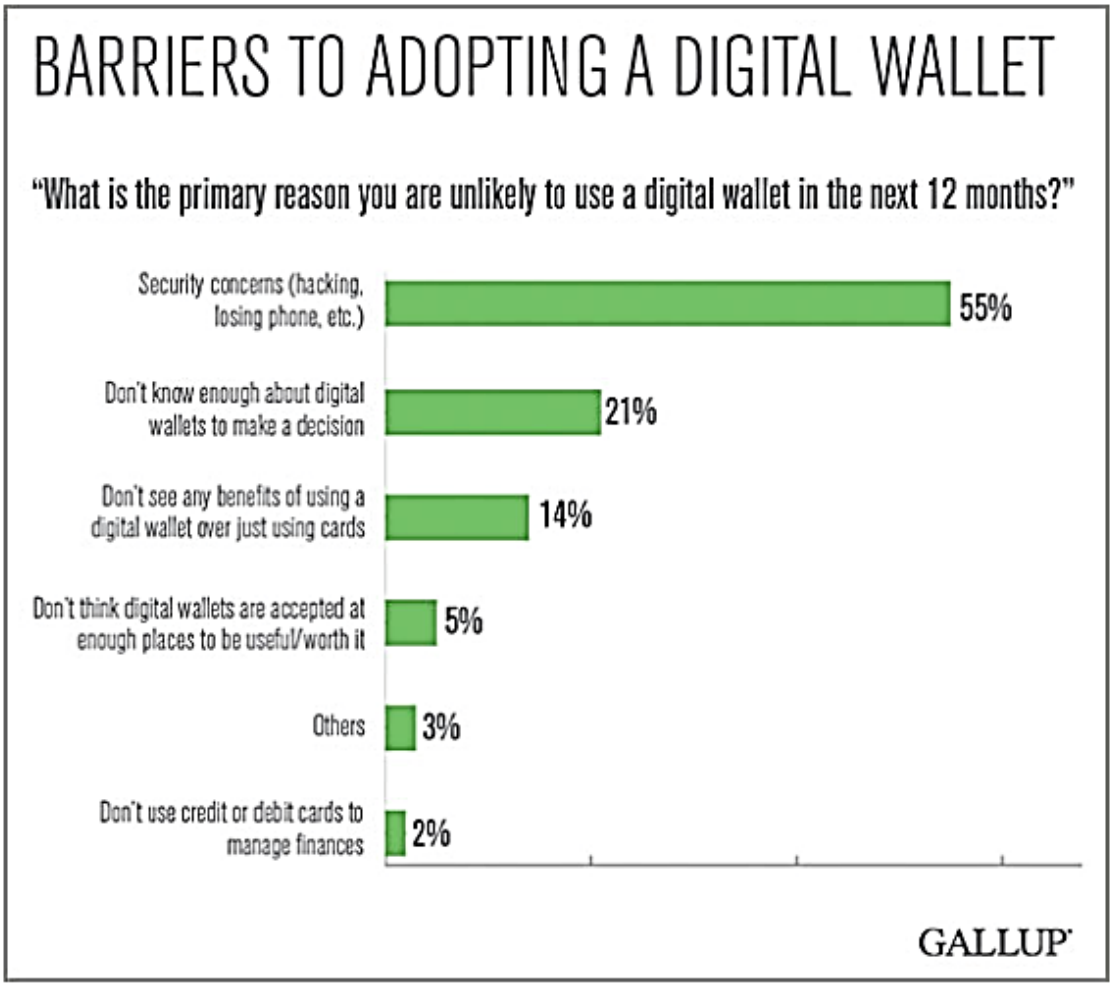
What is also interesting is that many payment technology innovations have their origins in security: Chip and Pin, Tokenization, NFC and other innovative technologies were introduced either together with security, or solely because of the need to address security.

Speaking with one of the mobile payments start-ups, they confirmed that as much as 80% - 90% of all of their releases are negatively impacted by security related issues. The impact comes from two sources: time to market delay of feature release, and scope reductions. What's interesting is that the team is comprised of professionals with a banking industry background, and therefore, risk analysis is a very natural part of the culture. Specifically, they noted that despite the strong pressure to release updates and patches to their product, they still continue to be uncompromising on the security and privacy issues, and continue to address them until everyone is satisfied with the proposed approach and solution, and risks are well understood.

Despite all of the efforts and the highest level of security, customer confidence and concerns over security can still have a strong effect. Even much loved and trusted Apple has had trouble achieving the anticipated levels of volume in launching their Apple Pay product,

due to security related concerns. In the 2015 Gallup survey shown in **Figure 30**, 55% of the consumers listed Security as the key concern around adoption of this new innovation.

Figure 30 – Barriers to adopting a digital wallet



Source: Gallup

Summary of the insights

- When technology-enabled innovation is driven by a highly competitive environment and fight for market share, cyber criminals may look to take advantage of the new opportunities and may choose to shift their activities to the new segments, although they will continue to exploit known vulnerabilities as well;

- Compliance plays a significant role and significantly advances the security agenda, but is not enough to protect a company's value, and therefore focus on compliance alone is not recommended as a best practice;
- When security concerns are transparent and widely publicized, they can lead to real or perceived lack of adoption of the new innovations;
- In the environments with high levels of fraud and high levels of regulation, security must be one of the key drivers of new innovations;
- Highly innovative firms with a mature security posture and strong risk management culture may experience a self-imposed negative impact on the innovation, in order to protect customers and company value.

Example of newer technologies: IoT (Internet of Things)

Value creation opportunities of IoT

According to Technopedia, "The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices." This trend is significant, because once again, it stands to revolutionize many industries and consumer interactions. Early implementations of IoT are connected cars and wearable devices that are already available today. However, we are still in the very early stages of the IOT revolution. Postscapes is one of the companies that is closely tracking various adoptions and implementations of the IoT technologies. According to Postscapes, as of the end of 2015 based on the latest group of tracked companies, the future of IoT can already be broken into the following categories:

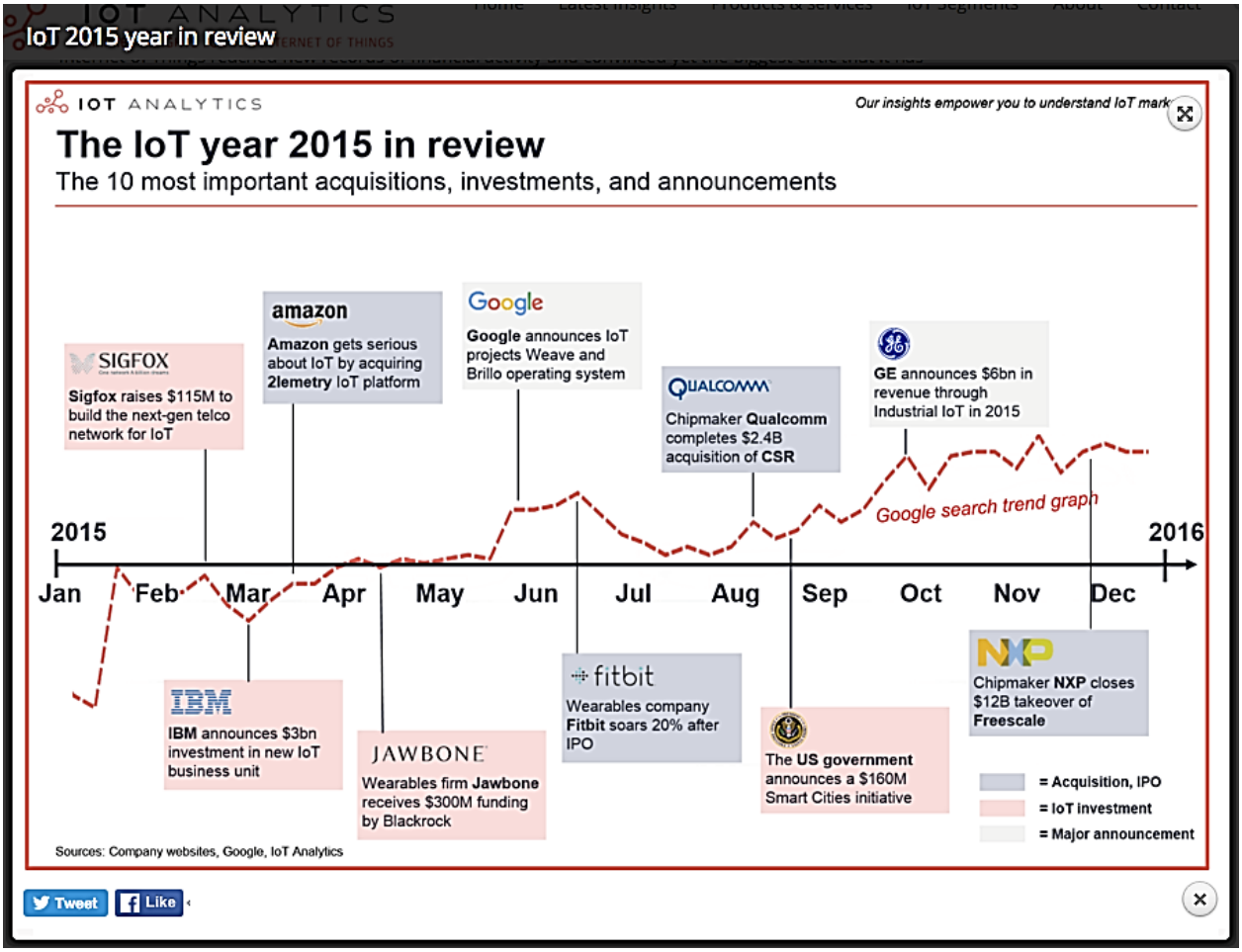
- IoT sensors used for our health. The related use cases would allow us to check on the baby, remind us to take medications, track our fitness activity, monitor ourselves and our relatives' health, and so on;
- IoT used in our homes will allow us to heat or cool our houses, monitor and control the usage of our appliances, monitor utility consumption, control the lights and even water our lawn;
- IoT used in our cities will allow us to streamline our waste disposal systems, improve traffic flows, monitor pollution levels, improve utility consumption and control the lights;
- In an industrial setting, IoT would allow companies to streamline and create efficiencies in maintenance and repair services, do A/B testing of the real products on the shelves, keep track of the assets and improve quality control functions;
- Finally, for the environment, IoT will help us monitor the pollution levels, track water supply, help protect wildlife, get advance warnings and so much more.

In reality, it's likely that this list is only the "tip of the iceberg" of the innovations that are truly possible with the introduction of the IoT. As mentioned in "The Second Machine Age" by

Erik Brynjolfsson and Andrew McAfee, modern technological progress is exponential, digital and combinatorial. When IoT technologies can be combined with Cloud Computing, Mobile, Big Data and Artificial Intelligence, the actual number of possibilities become infinite. The only real issue then becomes to find truly valuable ones, and extract maximum value from these combinations (p132).

To demonstrate the interest in the IoT trends, IoT Analytics has been tracking various investment activity in this space in 2015, which clearly shows strong interest from the tech giants, such as IBM, Google, Qualcomm, Amazon and others. According to this report, the IoT related M&A deals surpassed $20B in 2015 and startup funding reaching the $1B mark, marking new records of financial activity (Deans, David H, 2015).

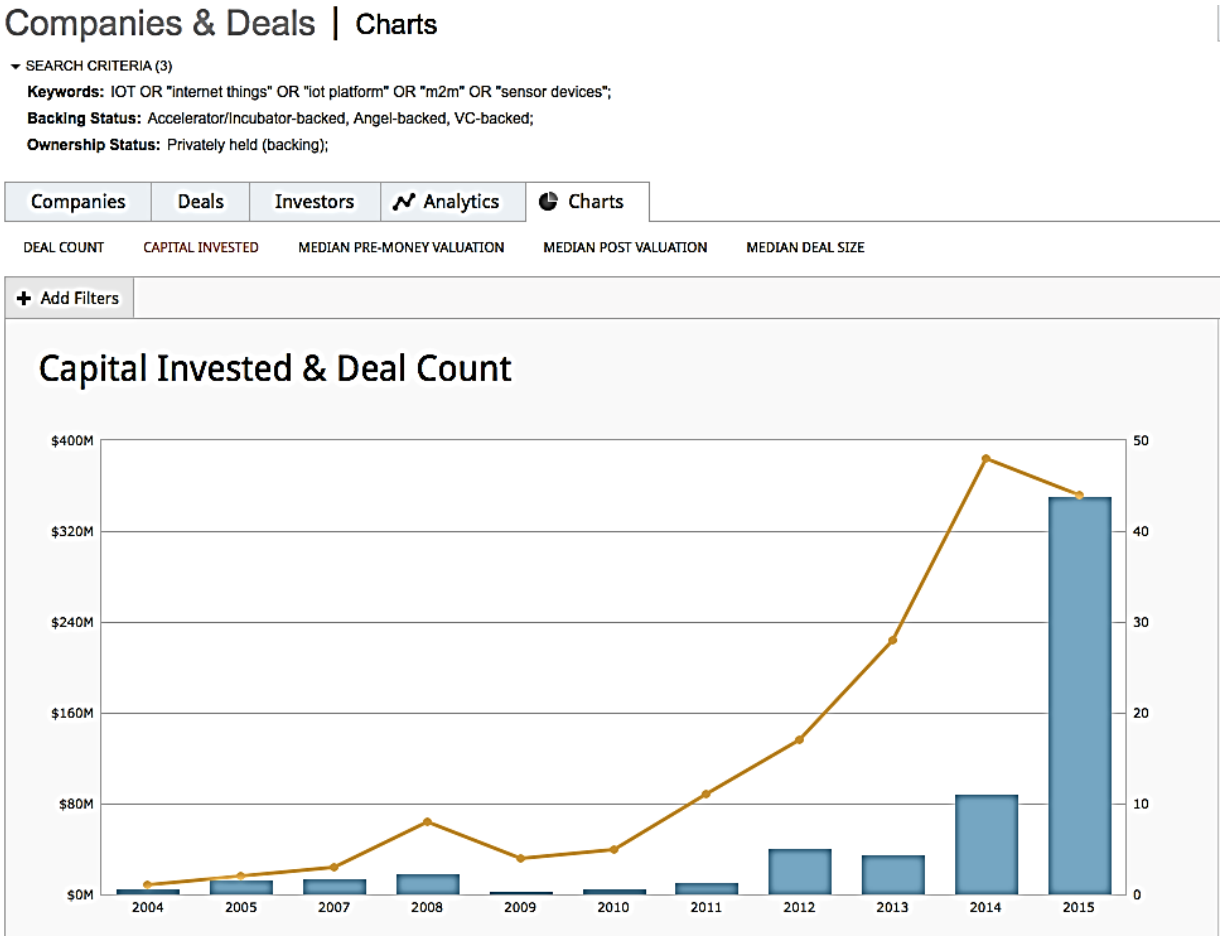
Figure 31 – the IoT year 2015 in review



Source – IOT Analytics

To further support the market's interest in the IoT and estimate anticipated value, we turn to the VC-backed deals trend over the last few years. Although the total value in 2015 is still relatively modest compared to other types of technologies, the trend clearly demonstrates growing interest in the potential value creation opportunities offered by the IoT technologies. This trend also shows that this is only a very recent development, as compared to more mature areas of technological innovation.

Figure 32 – Capital Invested and Deal Count for IoT



Source – Pitchbook (Zook—Aya, and Principal, 2016)

Possible cyber-risks of IoT

Once again, however, consumers, companies and economies are not the only ones looking to extract value from these innovations. Assuming that the aforementioned tools take hold and start adding value to the economy, we can begin contemplating potential value that hackers of different kinds would be interested to extract by either accessing the data or controlling the systems themselves. In Table 16 below I suggest possible scenarios of such

"matching" risks to hypothetical loss of value. Since we have very little or no data to support these hypothesis, companies that are developing products or services in these areas will need to examine the potential threats very carefully.

Table 16 – Possible Cyber-risks of IoT

Category of use	**Use Case**	**Potential value to hackers (for theft, espionage, state actors, or hacktivism)**
Vehicle	Maps & traffic guidance	Misleading to another location
	Entertainment systems	Not yet determined
	Unlock the car	Access to car
	Monitor for service & safety	Take control of the car
Health	Check on the baby	Health records fraud, ransom
	Remember to take medications	Health records fraud, ransom
	Track activity	Health records fraud, ransom
	Monitor effect of medication	Health records fraud, ransom
	Monitor ageing family member	Health records fraud, ransom
	Read Biometrics	Health records fraud, ransom
Home	Heat and cool the home	House vacancy information
	Monitor appliances	Not yet determined
	Track your keys and items	Access to house and valuables
	Control lighting	Not yet determined
	Monitor utilities	Access to house and valuables
	Monitor and control house plants	Not yet determined
Your city	Monitor waste	Not yet determined
	Optimize parking	Not yet determined
	Monitor pollution	Control of critical Infrastructure
	Monitor utilities	Control of critical Infrastructure
	Monitor and control lighting	Control of critical Infrastructure
	Share data with citizens	Not yet determined
Industry	Optimize maintenance and repairs	Control of production
	A/B testing of physical products on shelves	Corporate Espionage

	Monitor structural integrity	Control of critical Infrastructure
	Keep track of assets	Control of assets
	Monitor safety equipment (i.e. fire extinguishers)	Control of critical Infrastructure
	Quality control	Not yet determined
Environment	Monitor pollution levels	Control of critical Infrastructure
	Track utilities	Control of critical Infrastructure
	Help protect wildlife	Poaching
	Monitor for landslides	Not yet determined
	Monitor wildlife	Poaching
	Monitor deforestation	Illegal deforestation

According to the recent Gartner article "Gartner Says that the Internet Of Things Will Change Cybersecurity Forever", over 20 percent of enterprises will have digital security services devoted to protecting business initiatives using devices and services in the Internet of Things (IoT) by year end 2017. Since IoT technologies, combined with other big trends, will grow exponentially, the sheer size of the required cyber-security efforts in the IoT days will be much greater as compared to those required today. Also, since IoT innovations connect physical and digital worlds together, allowing each state to impact the other, the new cyber-security efforts will also have to "spill over" into the physical world, often requiring environment-specific or even device-specific defenses. Once again, the burning question is – how do companies balance the need to innovate with the need to secure?

Examples

To help answer this question, let's turn to a real life example from a North American based auto parts manufacturer and investigate how IoT innovations and related cyber-risks are being addressed, as based on the interview with their CIO.

The company's strategic operating model relies on 100% autonomous local businesses where choices and decisions are made by the local management team based on the local context. To maintain this operating model, the IT strategic plan called for building a "utility" IT platform that would centralize and standardize technologies without compromising any local decision making authorities. As a known consequence of this model, most of the IT systems are decentralized and heterogeneous, and current IT maturity is estimated generously at a 2 out of 5. "We are just standing ourselves up." As an unintended consequence there is proliferation of technologies and a lack of standards. As a result, it has led to 3 families of impairments:

1. Security – to secure a platform, company needs to implement IT standards. Since until recently there was no IT governance, implementing security measures became the #1 impairment of the autonomous strategy.
2. Scale – little economies of scale existed. With this diversity, achieving scale, which is the essence of modern IT, became the #2 impairment.
3. Finally, the company hardly had any cross-divisional capabilities. There are almost no analytics, no data warehouse, and no other cross-disciplinary capabilities, making it the third impairment.

The new IT Strategy is designed to address these areas:

- Phase 1: establish basic IT Utility – clean-up without compromising the operating model. Security will be a key element of this phase of the strategy.
- Phase 2: layer on cross-enterprise capabilities to start generating additional efficiencies and benefits. Many, many cross-divisional capabilities are being anticipated in this phase.

Governance structure:

- Utility technologies and security decisions will be driven by IT;
- Any new cross-divisional capabilities will be put forward and sponsored by a champion outside of the IT discipline;
- Security governance and risk management framework is important. There is security language in every RFP, and all new projects have a security component in them.

New innovations in IoT – manufacturing:

- In the manufacturing context, IOT-based innovations are being seriously considered, because world Class Manufacturing is one of the strategies of the company, with the specific focus to define smart, pragmatics ways of manufacturing;
- The manufacturing plant has an ERP, and a Manufacturing Execution System (MES), which does scheduling, raw material planning and interfaces with programmable controllers. MES necessarily deals with the IoT world – that's the sensor on the machine, and the Maintenance scheduled application.
- Because of decentralization and heterogeneity, there are currently multiple MES vendors and no way of addressing security. Therefore, until MES is standardized and secure, IoT innovations cannot be addressed.

New innovations in IOT – cars:

- In terms of Smart Cars and Driverless vehicles, the company worries a lot about these new innovations and is flirting with that side of the business;
- Due to the publicity of a recent vehicle breach, cyber security is top of mind in the product development;
- Manufacturer has recently acquired a company that specializes in cyber-security for the automotive systems;
- This segment of cyber-security is under the R&D umbrella and is not addressed by the IT group.

Tensions generated by cyber-security:

- There are many tensions within the organization. Global IT is a new construct with a mission to centralize certain aspects of IT. Due to the distributed locations, there are "manufacturing cowboys" who are used to having control over everything that happens in their branch;
- When applied to security, here are some of the examples that generate tensions:
    - Mandating passwords on the smartphones: "What do you mean I need this type of password? Apple doesn't require me to have this difficult of a password!"
    - Very immature environment, and consequently raising the awareness is a big problem and a big task;
    - Although people have heard of well-known attacks, such as Target, Home Depot and others, they somehow didn't internalize it and are surprised when they are now asked to consider cyber-security as a serious issue that applies to them.

Summary of the insights

- Loosely governed decentralized heterogeneous systems, frequently associated with a decentralized operating model, impair IT's ability to secure the environment. At the same time, they also impair the company's ability to innovate on a company-wide scale;
- A decentralized operating model also creates tensions due to lack of expertise in distributed locations: at the time of change, local operators use their consumer-based understanding of technologies to draw conclusions and make decisions, frequently resisting the required change;
- Adoption of the IoT-based innovations in manufacturing processes requires connection between the physical manufacturing technologies (OT) and the enterprise technologies

(IT). Manufacturers must first standardize and secure relevant IT systems. Without this standardization, value-creating innovations cannot be pursued;

-
- Adoption of IoT-based innovations into the product doesn't require connection to IT, and can therefore be pursued completely separately. This in essence expedites the innovation agenda, and allows for a faster time-to-market;
- Although breaches are frequently reported in the media, and most consumers have now experienced some level of fraud on their identity or credit cards, managers continue to disassociate these events with their own business risk, and don't see how something similar might happen to them.

Example of emerging technologies: Blockchain

Definition and the innovative potential of blockchain

Finally, I would like to say a few words about the newest set of technologies that are just starting to emerge now, and are based on the distributed ledger concept of Blockchain. I would like to use the definition

> "A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are replicated in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network. "

Blockchain technologies are promising to be very disruptive, especially in the ownership and financial services industries. So much so, that most major banks and several governments have started to invest in the development and prototyping efforts based on this technology, as means of figuring out new business models and become early adopters of the changes enabled by these technologies.

Thinking how to address cyber-security of blockchain

As companies and governments are examining possible future transformational innovations that these technologies will bring, I wanted to understand how they will think about the cyber-security implications, given something that is so new, and so disruptive.

Here are a few key points that I have learned in investigating the cyber-security implications of the blockchain technologies.

Due to the inherent design based on cryptography, distributed computing and the consensus mechanism, blockchain technology itself has an inherent trust mechanism that is promising to solve many cyber-security problems.

Having said that, due to it being so new, blockchain is likely to be exposed to "innovations" from the dark side and could itself be exposed to a number of new, still undiscovered cyber threats. There are a few examples of currently known issues or potential issues with this technology, but it is clear that more threats will emerge over time.

Currently, the Enigma (enigma.media.mit.edu) initiative that is being undertaken at the MIT Media Lab proposes a combination of the "off-chain" technologies with the blockchain technology, as a way of resolving trust issues and enabling identity management to support security.

There are other security concerns with the blockchain technology. According to Russian anti-virus provider Kaspersky, who has worked with Interpol on a proof of concept, "Blockchain Offers Safe Haven For Malware And Child Abuse". There are also concerns of hackers taking over more than 50% of the nodes on the chain. With these are other potential threats that are likely to emerge in the future. The real question for the firms is: if we want to take advantage of the new innovations offered by the emerging technologies, and given that the cyber-risks are opaque and not yet well understood, how should we approach this effort?

I've asked a number of major banking IT executives on how they think about it, and based on these discussions, could offer the following set of recommendations:

- First, companies should examine the options for potential partnerships that could help get started with the experimentation For example, consider partnering with MIT's Enigma project, IBM, Chain, ConsenSyss, Digital Asset Holdings or others, all of whom are focusing on the blockchain technologies;
- Forming these relationships and ensuring the exact alignment of incentives of all parties is extremely important. In these conversations, it is also important to understand their cyber-security approaches and include this in the partner selection process;
- To be able to leverage the opportunities of such cutting edge technologies, companies should also get actively involved in the blockchain development communities, such as standards development bodies and open source blockchain communities, to develop

strong internal technical expertise in this area, as well as getting a solid understanding of the technologies themselves;

- Once internal technical expertise is develop and strategic partnerships are identified, companies may want to start setting up development environments. For example, most banks currently set this up internally, using a "private" blockchain approach; although this approach is limiting the power of technology, it may be just a good first step;
- Security solutions should be created as a fundamental building block of any new blockchain based solution. Luckily, blockchain technology lends itself quite well to solving some of inherent problems with traditional databases, and solutions such as MIT's Enigma are emerging;
- Once some internal expertise is established and isolated proof of concept technologies have been developed, it is critical that cyber-security review and risk analysis be addressed. This step may potentially delay any implementation of the next steps, but it is even more critical given the opaque nature of cyber-risk associated with these new technologies. Only when cyber-risk is relatively well understood, accepted and mitigating solutions are designed and tested, can companies move towards implementation of these new technologies.

Chapter 8: Conclusions and Recommendations

The rapid pace of technological innovation is continuing to offer companies an unprecedented number of new value creation opportunities. The firms with a lower level of digitization are best positioned to reap the rewards from these innovations, and are accelerating their efforts to do so.

In parallel with these developments, cyber-security related threats are also escalating, and are forcing companies to increase their efforts and attention towards understanding and mitigating cyber risk.

Often, but not always, these two priorities are at odds with one another and companies are forced to make necessary trade-offs. Some companies are now starting to realize the strategic long term importance of addressing cyber-security as a core value, and are seeing it as a competitive advantage.

According to the findings of this research, however, only 13% of companies believe that they have found the right balance between the two priorities, and are experiencing relatively low negative impact on innovation imposed by the cyber-security activities.

It is also clear that some companies take on too much risk, often without fully realizing it, while others may not be taking full advantage of the available technology enabled innovation opportunities and may be leaving value on the table.

Generally, companies fall into these four main categories:

- 27.78% of the companies would be "below average" on both the "Technology Innovations" as well as "Cyber Security Maturity" measurements;
- 12.96% of the companies would be "below average" on the "Technology Innovations", but above average on the "Cyber Security Maturity" measurements;
- 29.63% of the companies would be "above average" on the "Technology Innovations", but below average on the "Cyber Security Maturity" measurements;
- 29.63% of the companies would be "above average" on both the "Technology Innovations" and the "Cyber Security Maturity" measurements.

The following factors may impact which category the company falls into:

- Industry environment;
- Company factors;

- Technology management practices;
- Technologies and their relative maturity.

Industry related factors impacting cyber-security posture and management are primarily related to the regulatory environment, innovation pressures and the publicity of cyber breaches. Since these factors are primarily external, they need to be well understood and incorporated into the overall company's cyber-security posture and related strategy. Company factors and technology management practices are those that companies have most control over. It is clear from this study, however, that these factors are the ones where we see the highest numbers of issues, specifically:

- Operating model and organization structure;
- Company culture and tensions created by cyber-security efforts;
- Board of directors and their role in cyber-security and innovation trade-off decisions;
- Education, communication and organizational awareness;
- Legacy architectures;
- IT governance and resource allocation.

Finally, the maturity of technologies considered for various innovation projects also plays a significant role in the amount of cyber-risk and how it gets addressed. Upon examination of the three types of technological trends, starting from more mature technologies, such as electronic payments, to new technologies such as the Internet of Things, and to the emerging technologies such as Blockchain, we see that the role of cyber-security will become a key foundational building block upon which new levels of trust in the new digital economy will be built.

Those companies that take security seriously and address it at the industry, company and technology levels, will be well positioned to not only protect the existing value of their company, but create new value as cyber-security gets built into all new innovative technologies at the foundational levels.

Practical recommendations

Based on this research, I would offer the following simple set of steps to CIOs and CISOs, as they review these results:

- Using the same questions as were posed in the survey, evaluate which quadrant the company is in, and compare with their risk and innovativeness profile in other parts of the company.
- Adjust for the industry factors and the company's inherent risk posture to see which quadrant would be most appropriate for your firm in the short and long run. If there is no current cyber-security regulation or such regulation is not enforced, the company may be exposed to a weaker security posture; this should become a subject of a strategic discussion with the board.

- Evaluate board and senior leadership support; use frequency, length and interactivity of the board cyber-security briefings as a proxy to compare against others in this study.
- Examine cyber-risk measurement practices; specifically, ask whether the risk is measured, how often it's measured, whether it's used for the purposes of accountability, strategic planning, budget approval or any other purposes.
- Check for possible misaligned incentives in the organization structure; this will be especially relevant for companies with high competitive pressures to release new digital products and solutions – in these cases, if product managers are not ultimately responsible for the security of these products or solutions, an unintended set of risks might be created.
- Check for the culture, education and awareness at all levels. For example, pay specific attention to the technical education of the development teams and the education of any executives that could become victims of ransomware as well as the broader employee population who could be targeted for social engineering.
- Ensure strong technology management and governance practices.

Appendix

Survey Questions

1. Region: Please identify the primary region where Innovation Projects are approved in your organization or organizational unit

#	Answer
1	Europe / Middle East / Africa
2	North America
3	Asia / Pacific
4	Latin America / Caribbean

2. Please identify your industry / sector

#	Answer
1	Banking and Financial Services
2	Government - State/Local
3	Government - National / International
4	Professional Services
5	Insurance
6	Retail and Wholesale
7	Software Publishing and Internet Services
8	Education
9	Construction, Materials and Natural Resources
10	Industrial Manufacturing
11	Transportation
12	Energy
13	Utilities
14	Pharmaceuticals, Life Sciences and Medical Products
15	Telecommunications
16	Travel and Hospitality
17	Food and Beverage Processing
18	Healthcare Providers
19	Media and Entertainment
20	Industrial Electronics and Electrical Equipment
21	Chemicals
22	Other

3. Please select what best describes your role in the organization

#	Answer
1	Board Member
2	CEO
3	CIO
4	CISO
5	CFO
6	Marketing Executive
7	Operations Executive
8	VP of IT
9	IT Director / Manager
10	Other

4. Number of employees in your organization

#	Answer
1	Fewer than 1,000
2	1,000 to 9,999
3	10,000 or more

5. Technology enabled innovation projects: In the last twelve months, to the best of your knowledge, approximately what percentage of value-creating, innovative projects undertaken by your company or organizational unit were empowered by or enabled by technology? Value creation typically comes from projects that generate revenues, save costs, generate efficiencies, improve customer experience or improve product.

Select examples of value creating technology enabled projects:
- Mobile Applications for customers or employees
- Cloud Computing Services and Data center cost reduction projects
- ERP, Human Capital Management or Supply chain systems
- E-commerce or Mobile Commerce
- Internet of Things Projects
- Big Data or Business Intelligence projects

6. Impact of cyber-security concerns: Of all of the technology-enabled projects, in the last twelve months, to the best of your knowledge, what percentage was impacted by either real or perceived concerns of cyber-risks?

Example of such impact A bank has launched a mobile application for their customers on the IOS / I-Phone platform, but has delayed the release of an Android version of the application for three years due to concerns over the cyber-security of that platform.

#	Answer
1	Percentage of all projects delayed due to cyber security
2	Percentage of all projects cancelled due to cyber security
3	Percentage of all projects where scope was reduced due to cyber security concerns

7. Measuring cyber risks: To the best of your knowledge, in the approval process of these technology-enabled initiatives, what percentage of them included quantified risk analysis, including measured cyber-risk?

Examples of measurable risk analysis:
- Estimated percentage of defective parts, and associated replacement costs
- Number of late deliveries and associated costs

#	Answer
1	Percentage of projects with quantified overall risk analysis
2	Percentage of projects with quantified cyber-risk analysis

8. Board Briefings: Please share some insights into the frequency, length and depth of the Board education on the subject of cyber-security.

9. Cyber-security Reporting structure: Please identify who cyber-security unit reports to within your organization

#	Answer
1	Board of Directors
2	CEO
3	CFO
4	CIO
5	Legal
6	Other

10. Organizational characteristics associated with achieving the satisfactory balance of technology-enabled innovation and cyber-security efforts : Please describe any organizational or structural tensions, challenges, support networks or alliances that exist when addressing decisions on technology enabled innovations and corresponding cyber-risk analysis.

Examples:

- IT infrastructure and Operations IT teams have different priorities
- Projects get approved by various business disciplines without consulting with the IT Security team, causing delays, scope increases within projects or increased costs
- IT security team is short on resources

11. Specific examples: Knowing that your company's name will not appear anywhere, would you be willing to share one or more examples where you believe either too much cyber-risk was taken on without proper evaluation, or conversely, potentially very valuable projects did not go through due to real or perceived threats of cyber security issues? We are specifically looking to understand the environment, the underlying reasons, motivations and economic implications of such examples.

12. Willingness to be contacted in the future: Would you be willing to share your contact information with us, only for the purposes of any follow up questions and clarification, and with the continuing confidentiality? If so, please provide us with your contact information.

#	Answer
1	Yes, you can contact me for more details
2	Not at this time

13. (Optional) Survey results will be published and distributed. Any personally identifiable information will never be published or shared. Non-identifiable data may be shared with industry associations. Please provide your consent to complete this survey.

#	Answer
1	I give my consent to share non-identifiable information and results of this survey combined with responses of others

Responses to the question of Organizational Characteristics and Tensions associated with balancing innovations and cyber-security priorities

These are complete responses to the following question:

Organizational characteristics associated with achieving the satisfactory balance of technology-enabled innovation and cyber-security efforts

Please describe any organizational or structural tensions, challenges, support networks or alliances that exist when addressing decisions on technology enabled innovations and corresponding cyber-risk analysis.

Examples
IT infrastructure and Operations IT teams have different priorities
Projects get approved by various business disciplines without consulting with the IT Security team, causing delays, scope increases within projects or increased costs
IT security team is short on resources

Response
We are a startup engaging in renewable energy business. At the moment, we spend quite little time on cyber-risk analysis.
There are too many "shadow IT" projects within the company due to a lack of IT resources. We've also realized that to get the best cyber protection we need to leave it to the experts therefore we've outsourced our cyber security efforts and management.
The Group working with cyber-risk has been limited but growing during 2015. Focus and efforts has increased drastically. The interest from top level have had a strong impact on activities. A CISO has been appointed and resources within IT fully focusing on Security has increased. The initiatives has so far not put many restrictions on developing and using new technology. Education and awareness has been prioritized.
Shadow IT sources technologies without IT involvement lack of appreciation for IT security risks lead to uninformed decisions
Security is a complex issue that comes at a cost, and when scrutinizing costs or trying to deliver projects timely, even the most loyal of supporters have a hard time believing the security "guy". Security is one of the areas because of "belief" or complexity regularly required 3rd party "neutral" spend to get the commitment to progress. Making it more costly and time consuming.
Projects get approved by various business disciplines without consulting with the IT Security team, causing delays, scope increases within projects or increased costs.

Projects do not consistently plan for security considerations and they are incorporated late into initiatives. Business groups want to avoid security practices that impact customers/conversion where IT wants to push for heavier security requirements. Costs of security features can impact the approval of projects. Support from vendors is not always at a sufficient level where security is concerned (they are trying to catch up on security standards as well). Internal expertise on security is lacking and under resourced. Security projects involve large amounts capital and typically need require ongoing operating support to maintain; both of which are limited in an organization.
Poor resources of IT teams
Poor alignment between field operation on business side 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. Business opportunities are lost due to conservative security policies and lack of appetite for more transformative digital development initiatives.
Our IT security team always works with other IT team so that they can identify undefined potential risk. Since IT and Operation teams are managed by two different managers, sometimes it takes too much time to make one simple decision relating both divisions.
Our company is risk averse. So we set specific and organized rule to execute digital marketing. Therefore, there are not many cases where we have to face cyber security. However, the guideline was defined in 10 years ago. So it seems outdated. We should revise it, but, due to the drastic technological change, It is difficult to catch up with all of the trends. This is our challenge.
Our big clients were financial institutions so they took cyber risk very seriously. When I left the company, we were looking into hiring outside firms to try and break in / hack our system to ensure it was secure. It was costly and we were a small shop, so we were fighting having to pay for the whole thing.
Not really vivid threat explanation which impacts the business operation.
No major issues. On occasion my Corporate Security Officer and her team take a bit too long to do a proper cyber-security evaluation.
No IT security team.
Many projects can't be realized due to strict regulation and increasing risks, especially in financing industry in Japan. We can't utilize even cloud services to protect customer information.
Manufacturing Area is relatively less exposed to the cyber risk and thus, it is challenging to raise the priority of management for the cyber risk.
I will keep all the examples you gave as my examples.
IT team and customer service team have different requirement, so the system is delayed.

IT security uses a "cookie cutter" risk approach, most of which is addressed by standards set in IT infrastructure. Little is done to inspect the PRODUCT being deployed onto that infrastructure other than saying "make sure you use 128 bit encryption!!". This being said, the IT Security still manages to take time out of projects to properly "assess" them for seemingly no value.
IT security team limits the potential of IT in improving efficiency due to cyber security concerns.
IT security team is short on resources.
IT security is embedded within the IT team, so this tension is more about IT vs project work. We focus and have rejected scope from business-driven projects due to risk.
IT security and IT operations do not coordinate or share information Many projects proceed without considering IT security issues IT security team is very short on resources and training There is a tendency to not report cyber incidents or to downplay the extent or seriousness of the incidents as it would refect poorly on the IT security head Cyber risk is a risk covered by the Risk Management Committee which reports to the board but insufficient information is provided to the Committee
Its a join and collaborative decision making with IT Security, IT Apps and Infrastructure all aligned with common goals. Security is never an after thought.
IT dep are responsible for tech security Business units are responsible for information security(what's in the systems) Sometimes this creates a Greyzoon between the two units.
in one company they felt that the spending could be a black hole so didn't want to spend hardly anything hard to find the qualified staff to trust on what is the right spend and hard to qualify the hiring of staff to find these holes
Information Security serves as a consultant to internal organization. It is the responsibility for other non Information Security teams to implement the controls. This requires a higher staffing level in IT to achieve the desired risk level. Information Security is adequately funded but IT can't keep up with demands.
First two examples apply to us
External vendor partners that are part of combinatory solutions have their own frameworks/timelines. Business team members understanding the actual IT risks are and their related impacts.
Business Relationship Management (BRM) dirves proojects to quick completion, security introduces delays that are sometimes not welcome.
Any new IT project has to be reviewed by IT Security before launch Our IT team is very responsive
Although recognized as a potential threat to the well being f the organization, the inability to quantify the degree of the damage allows management the luxury of delaying adequate deployment of resources.

Advance planning team wants to use customer information as much as we can. However, the conventional executives usually block them due to legal problem. Legal team is short on resources to survey the legal problem on cyber-security issues. So, we always select a least risk choice.

Bibliography

Works Cited

Computer Business Review. *Dealing With Declining Digital Trust Among Consumers*. Oct. 2015. Web. 17 Oct. 2015.

KPMG International. "Cyber security: a failure of imagination by CEOs." *kpmg.com/CEOOutlookCyber*. KPMG, 11 Feb. 2016. Web. 30 Apr. 2016.

MIT CISR. *Digital disruption and the role of IT leadership « center for information systems research - MIT Sloan school of management*. n.d. Web. 25 Apr. 2016.

Ponemon Institute©. *20151 Cost of Data Breach Study: Global Analysis*. 27 May 2015. Web. 25 Jan. 2016.

Postscapes. *Tracking the Internet of things: Postscapes*. Postscapes, n.d. Web. 25 Apr. 2016.

"Accenture technology vision 2015: Digital Business Era: Stretch Your Boundaries." N.p.: Accenture, 2015. Web. 25 Apr. 2016.

Afshar, Vala. "6 Ways to Build for Digital Change." (2015): n.pag. Web. 5 Apr. 2015.

"An expert perspective: Art Coviello on the board's role in Cybersecurity." *Spencer Stuart*. 27 Feb. 2015. Web. 31 Dec. 2015.

Andrus, Danielle. "Cybersecurity 'Not designed for the human Psyche.'" Google Plus, 3 Feb. 2016. Web. 5 Feb. 2016.

Barefoot, Jo Ann. *Harvard and Hogwarts: Magic for the payment system*. Jo Ann Barefoot, n.d. Print. 30 Apr. 2015.

BBC. "Uber Error Leaks US-Based Drivers' Data." *BBC Technology* 14 Oct. 2015. Web. 25 Dec. 2015.

---. "US Airline to Reward Bug-Finding Hackers." *BBC Technology* 15 May 2015. Web. 17 May 2015.

Benner, Katie. "With a Mobile Website Like an App, Flipkart Takes a Swipe at Apple." *Bits* 9 Nov. 2015. Web. 9 Nov. 2015.

Cellan-Jones, Rory. "Stephen Hawking Warns Artificial Intelligence Could End Mankind." *BBC Technology* 2 Dec. 2014. Web. 10 Oct. 2015.

"Cover story: Top ten differences between ICS and IT cybersecurity." June 2014. Web. 5 Jan. 2016.

Crosman, Penny. "Biometric Tipping Point: USAA Deploys Face, Voice Recognition." 2 May 2016. Web. 27 Feb. 2016.

"Cyber-Security Stocks: Getting In Early – Everything You Need To Know." *Business*. ValueWalk, 7 Sept. 2015. Web. 7 Sept. 2015.

"Cyril Roux: Cybersecurity and cyber risk." 2 Oct. 2015. Web. 20 Jan. 2016.

Deans, David H. "IoT 2015 in review: The 10 most relevant news of the year." *IoT Market analysis*. IoT Analytics - Market Insights for the Internet Of Things, 23 Dec. 2015. Web. 31 Dec. 2015.

Elliott, Megan. "Can Apple Save the Digital Wallet?" *The Cheat Sheet*. The Cheat Sheet, n.d. Web. 26 July 2015.

Evans, Nicholas D., et al. *The cybersecurity needs of the borderless enterprise*. Computerworld, 27 Nov. 2012. Web. 11 May 2015.
Evans, Nicholas D., Disruptive Technology By Nicholas D. Evans Follow, and was one of Computerworld's Premier 100 IT Leaders. *SMAC and the evolution of IT*. Computerworld, 9 Dec. 2013. Web. 11 May 2015.
Ferrazzi, Keith. "Getting Virtual Teams Right." *Leading teams*. Harvard Business Review, 1 Dec. 2014. Web. 10 Oct. 2015.
Flows, Capital. "Disrupting Consumer Financial Services." 10 Sept. 2014. Web. 30 Apr. 2015.
---. "Disrupting Consumer Financial Services." 10 Sept. 2014. Web. 30 Apr. 2015.
Forrest, Conner. *The 10 most important lessons IT learned in 2015*. TechRepublic, 17 Dec. 2015. Web. 22 Dec. 2015.
"Fortinet launches worldwide network security academy to create global pipeline of Cybersecurity talent." Yahoo Finance, 22 Mar. 2016. Web. 23 Mar. 2016.
Garner, Luke. *Warning from Millennials: tighten online security or lose our custom*. 31 Aug. 2015. Web. 1 Sept. 2015.
Gartner. *Gartner says that the Internet of things will change Cybersecurity forever*. 2 Sept. 2015. Web. 25 Apr. 2016.
"Global Retail E-Commerce Keeps On Clicking." n.d. Web. 7 Apr. 2015.
Golden, Bernard. *5 IT industry predictions for 2016 from Forrester and IDC*. CIO, 20 Nov. 2015. Web. 25 Apr. 2016.
HM Government. *Distributed Ledger Technology: Beyond Block Chain A Report by the UK Government Chief Scientific Adviser*. 2015. Web. 25 Apr. 2016.
itnewsonline. *Gartner: Internet Of Things will Change Cybersecurity Forever*. n.d. Web. 6 Sept. 2015.
Kassner, Michael. *Cybersecurity professionals: The healthcare industry needs you*. TechRepublic, 28 Nov. 2015. Web. 1 Dec. 2015.
Landi, Heather. *GAO: DoD, VA need to improve Interoperability efforts*. 2 Nov. 2015. Web. 4 Nov. 2015.
Levitz, Eric. "Elon Musk and Stephen Hawk call for a ban on autonomous weapons." *MSNBC*. MSNBC, 28 July 2015. Web. 28 July 2015.
Levy, Oren. *A Guide to International Payment Preferences*. Entrepreneur, 24 Apr. 2015. Web. 25 Apr. 2015.
Lohrmann, Dan. *The top 16 security predictions for 2016*. 27 Dec. 2015. Web. 31 Dec. 2015.
McCandless, David. *World's biggest data breaches & hacks*. 2016. Web. 1 May 2016.
McGeer, Bonnie. "Accept It: The Blockchain Will Be Part of Your Bank's Business." 15 June 2016. Web. 7 Jan. 2016.
McKinsey. *Digital America: A tale of the haves and have-mores*. McKinsey & Company, Dec. 2015. Web. 25 Apr. 2016.
---. *Unlocking the potential of the Internet of things*. McKinsey & Company, June 2015. Web. 25 Apr. 2016.
Meola, Andrew. "This one chart explains why cybersecurity is so important." *Business Insider*. Business Insider, 16 Mar. 2016. Web. 18 Mar. 2016.

Metz, Cade, and Money. "Nobody knew how big a deal the cloud would Be—They do now." *Business*. WIRED, 22 Dec. 2015. Web. 8 Jan. 2016.
"Munich security report - Munich security conference." 29 Jan. 2016. Web. 30 Jan. 2016.
Peterson, Andrea. "Hackers Caused a Blackout for the First Time, Researchers Say." *Washington Post* 5 Jan. 2010. Web. 6 Jan. 2016.
Poblet, Marta, et al. "How cybercrime has evolved over the past 5 years." 7 Sept. 2015, Web.
pymnts. *Where fraud is looking Post-EMV*. PYMNTS.com, 9 Dec. 2015. Web. 9 Dec. 2015.
Ramsinghani, Mahendra. *Cockroaches versus unicorns: The Golden Age of Cybersecurity startups*. TechCrunch, 6 Jan. 2016. Web. 8 Jan. 2016.
Reserved, Kaspersky LabAll Rights. *Bitcoin's Blockchain offers safe haven for Malware and child abuse, warns Interpol - Forbes*. 27 Mar. 2015. Web. 25 Apr. 2016.
Reuters. "Cyber security startups face funding drought." *Tech*. Fortune, 24 Feb. 2016. Web. 23 Mar. 2016.
---. "TalkTalk Hacking to Be Subject of Inquiry on Cybersecurity in British Parliament." *International Business* 5 Nov. 2015. Web. 6 Nov. 2015.
russell.brandom, and Russell Brandom. "A New Experiment Tracks Credit Card Data as It Travels Through the Criminal Web." (2015): n.pag. Web. 8 Apr. 2015.
Salim, Hamid M. *Cyber safety: A systems thinking and systems theory approach to managing cyber security risks*. Massachusetts Institute of Technology, 2014. Web. 12 May 2016.
Savvides, Lexy, and Laura Hautala. *Laura Hautala*. CNET, 30 Dec. 2015. Web. 31 Dec. 2015.
Schwab, Klaus. *World economic forum annual meeting 2016*. World Economic Forum, 19 Apr. 2016. Web. 25 Apr. 2016.
Shontell, Alyson. "GM explains why it gave Lyft — a startup that wants people to stop buying cars — $500 million: 'Our business has changed more in 5 years than in the 50 years prior.'" *Business Insider*. Business Insider, 4 Jan. 2016. Web. 12 May 2016.
Siderwicz, Marilyn. *Pushing engineering boundaries to spur infrastructure innovation*. MIT News, 22 Dec. 2015. Web. 25 Dec. 2015.
Stalder, Dana. *The First Battle In The Mobile Payments War Is Over*. TechCrunch, n.d. Web. 1 June 2015.
Stark, Erika, Calgary Herald More from Erika Stark, and Calgary Herald. *Update: Police discover bogus credit cards used by renters of trashed Airbnb rental home*. Calgary Herald, 7 May 2015. Web. 10 May 2015.
"The CISO of Bombardier on Target, Sony and the changing nature of risk." IT World Canada, n.d. Web. 4 Sept. 2015.
"The Second machine age." The Second Machine Age, n.d. Web. 5 Jan. 2016.
"Trustonic and Mobeewave partner to give unprecedented security level in mobile payments." Cambridge Network, n.d. Web. 17 Apr. 2015.
Urrico, Roy. *10 biggest data breaches of 2015*. n.d. Web. 7 Jan. 2016.
---. *Payment Innovation Outpacing Security: Study*. n.d. Web. 29 Apr. 2015.
"What's Your Security Maturity Level? — Krebs on Security." n.d. Web. 27 Apr. 2015.
Wilson, David. "Technology Spending Sustains Citi's 'Raging bull' on U.S. Stocks." 17 Dec. 2015. Web. 7 Jan. 2016.

World Economic Forum, Pepper and Garrity. *1.2 – ICTs, income inequality, and ensuring inclusive growth*. Global Information Technology Report 2015, 2016. Web. 25 Apr. 2016.
Xu, Kevin. "Protecting Payments in 2015: Exclusive Q&A With PCI SSC's Stephen Orfei." (2015): n.pag. Web. 2 Apr. 2015.
Zetter, Kim. "Everything we know about Ukraine's power plant hack." *Security*. WIRED, 20 Jan. 2016. Web. 12 May 2016.
Zook—Aya, and Principal. *M&A, private equity & venture capital database*. 2016. Web. 12 May 2016.

Citations, Quotes & Annotations

"The Second machine age." The Second Machine Age, n.d. Web. 5 Jan. 2016.

> "The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices." ("The Second Machine Age")