MIT MANAGEMENT
SLOAN SCHOOL

INTERDISCIPLINARY
CONSORTIUM
for IMPROVING
CRITICAL
INFRASTRUCTURE
CYBERSECURITY
(IC)³

Trade-offs between digital innovation and cyber-security

Natasha Nelson
Stuart Madnick

Working Paper CISL# 2017-03

March 2017

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

Trade-offs between digital innovation and cyber-security

Natasha Nelson
Stuart Madnick

March 2017

MIT Sloan School of Management

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 cybersecurity 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 cybersecurity of their existing and new digital assets.

Therefore, 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 paper 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 cybersecurity maturity matrix. This positioning is then overlaid with the perceptual negative impact of cybersecurity controls on the innovative projects. The paper then analyzes the industry level, firm level, technology management and the technology maturity factors that affect this perception and these trade-offs. Ultimately a set of practical recommendations is provided to help a company to evaluate its own positioning on the innovation / cybersecurity matrix, understand the underlying factors that affect that position, and how to better manage these trade-offs.

Table of Contents

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), "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 in Table 1 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 1 – 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.

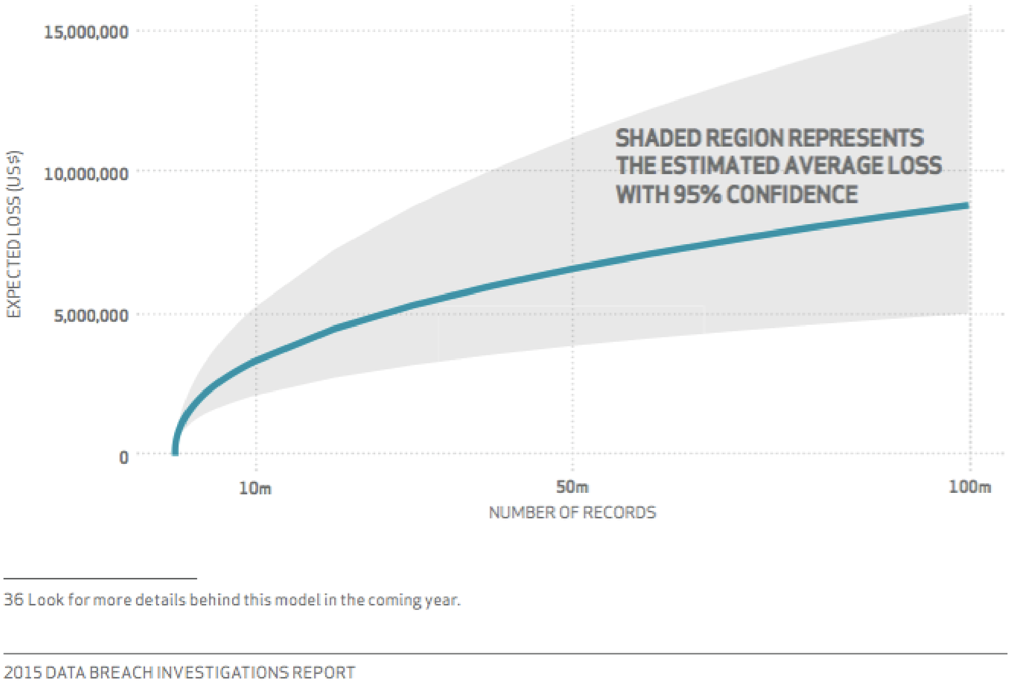
Negative impact of cyber-security related losses

On the other hand, many CIOs continue to maintain the responsibility for the on-going management of the cyber-security efforts. As a result, 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 1 below demonstrates these calculations.



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

2015 DATA BREACH INVESTIGATIONS REPORT

Figure 1 - Expected average loss by records lost

To further explore the number of breaches, their size and frequency, the "Information is Beautiful" website has put together the infographic shown in Figure 2.

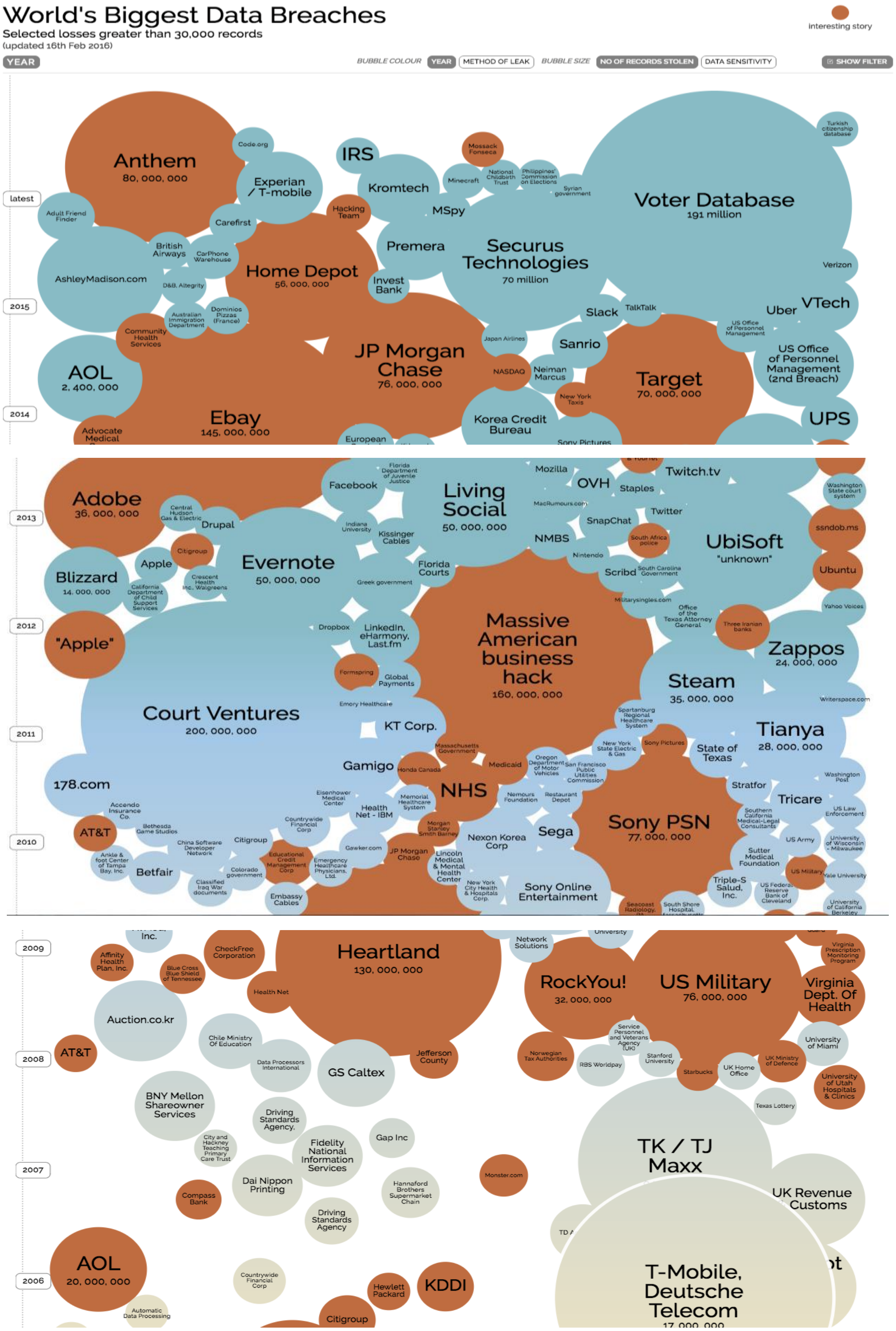


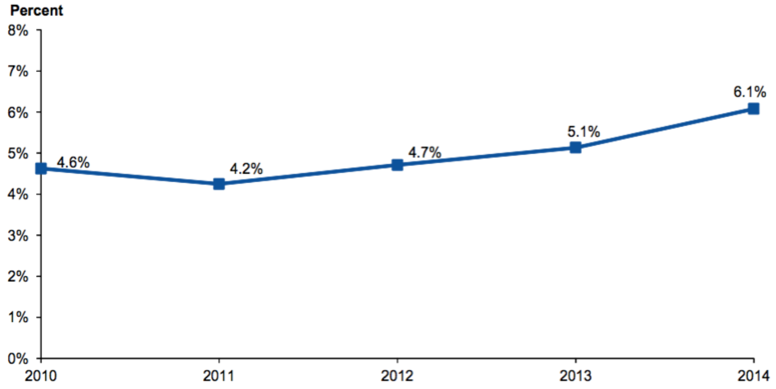
Figure 2 – World's Biggest Data Breaches

Source – Information is Beautiful

As we can see from that 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 recent ones at 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 3. 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.



Source: Gartner IT Key Metrics Data (December 2014)

Figure 3 – Total IT Security Spending as a Percent of IT Spending, 2010 – 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.

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 <u>tension between meeting the needs of the user and adding features that make money</u>. 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 sections will help examine these tensions both quantitatively and qualitatively.

Quantifying the impact of cyber-risk management on innovation

Initial framework and hypothesis

To examine the relationship between different factors and related trade-offs, this project started by building a simple framework (see Figure 4) that divides 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.

This framework was used to examine which companies would fall into various quadrants, and find underlying factors that would move companies into those quadrants.

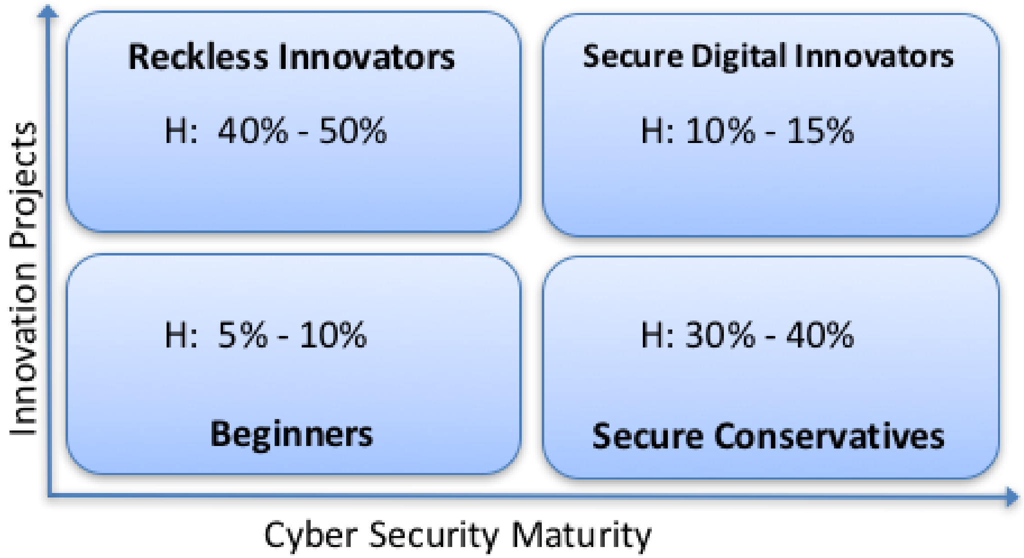


Figure 4 – Cyber Security Maturity and Innovation matrix

Based on intuition, experience and on-going monitoring of the articles on a variety of related subjects, the following situation was hypothesized:

- 5% - 10% of the companies would be "below average" on both the "Technology Innovations" as well as "Cyber Security Maturity" measurements; this group is called "The Beginners";
- 30% - 40% of the companies would be "below average" on the "Technology Innovations", but above average on the "Cyber Security Maturity" measurements; this group is called 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; this group is called the "Reckless Innovators";
- 10% - 15% of the companies would be "above average" on both the "Technology Innovations" and on the "Cyber Security Maturity" measurements; this group is called the "Secure Digital Innovators".

One of the goals of this research was to test these hypotheses and see what percentage of companies surveyed actually 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.

Analysis of survey respondents

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

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

Some basic demographic facts about the survey are provided in Tables 2, 3, and 4:

Table 2 – Survey Responses by region and industry

	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 3 – 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 4 – Survey Responses by region and 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, it was necessary to address the fact that both cyber-security maturity and the level of technological innovations within companies are not a well measured or commonly measured metrics. As such, questions were created that served as proxies to these measures. To ensure maximum accuracy, two specific survey techniques were used:

- 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.

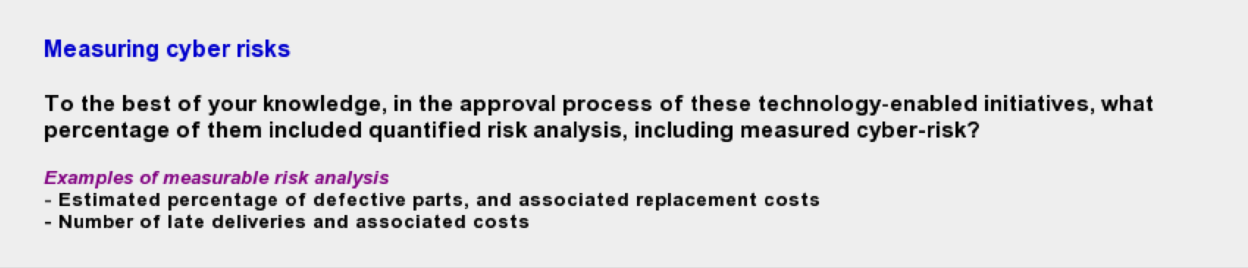
The results on a question by question basis are reviewed in the following sections.

Cyber-risk measurement

Who is measuring cyber-risk and why

For the proxy of "cyber security maturity" on the X axis of the framework, the notion of cyber-risk measurement was used: 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. The results of the risk-measurement question are shown in Table 5 and Figure 5.

Table 5 – 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

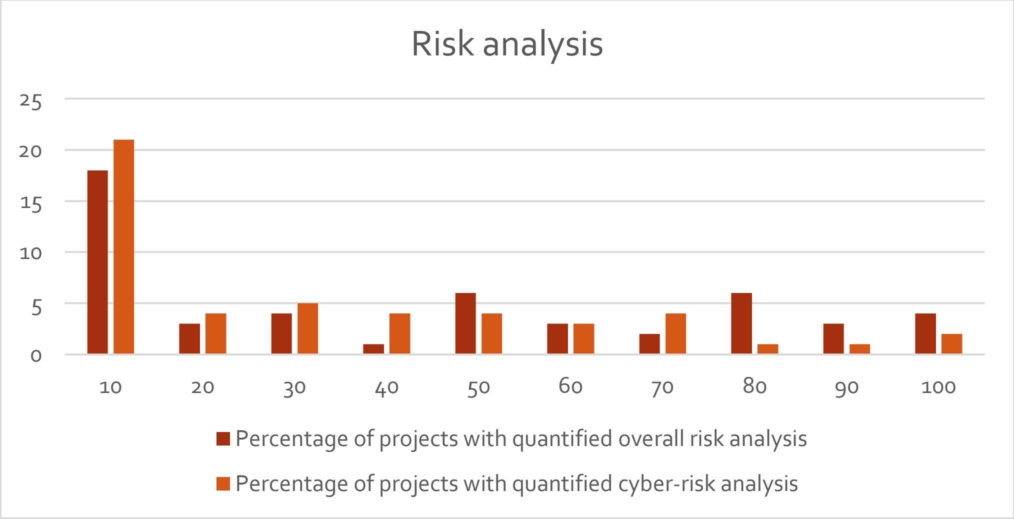


Figure 5 – Risk analysis

From the data shown in Figure 5, we can see that overall risk measurement on projects is not a common practice, 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 section). 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

The spectrum of the cyber-risk measurement practices is demonstrated by 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

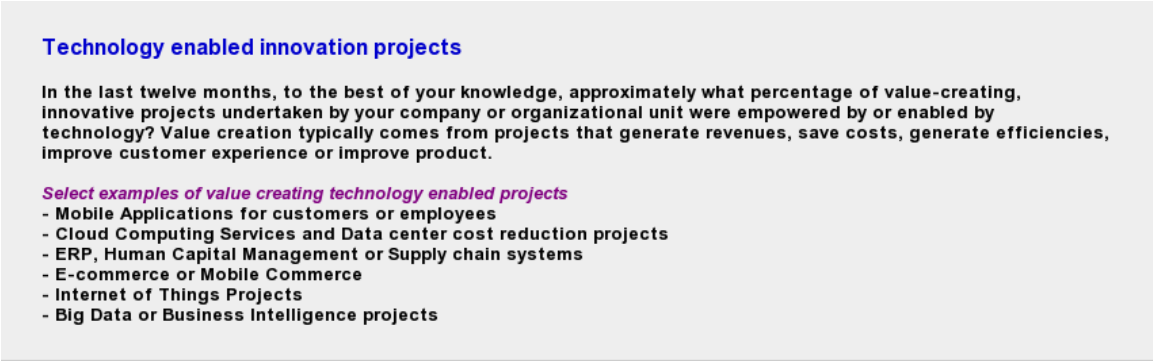
- Although there is currently no standard in cyber-risk measurement and reporting, a variety of approaches exists and is being used actively, adding transparency and efficiency;
- Measurements that are easily understandable and are actively discussed at the board meetings are most effective;
- Those 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, the percentage of innovative, value creating projects enabled by technologies was used. 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.

The results of the innovation measurement question are shown in Table 6 and Figure 6.

Table 6 – 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

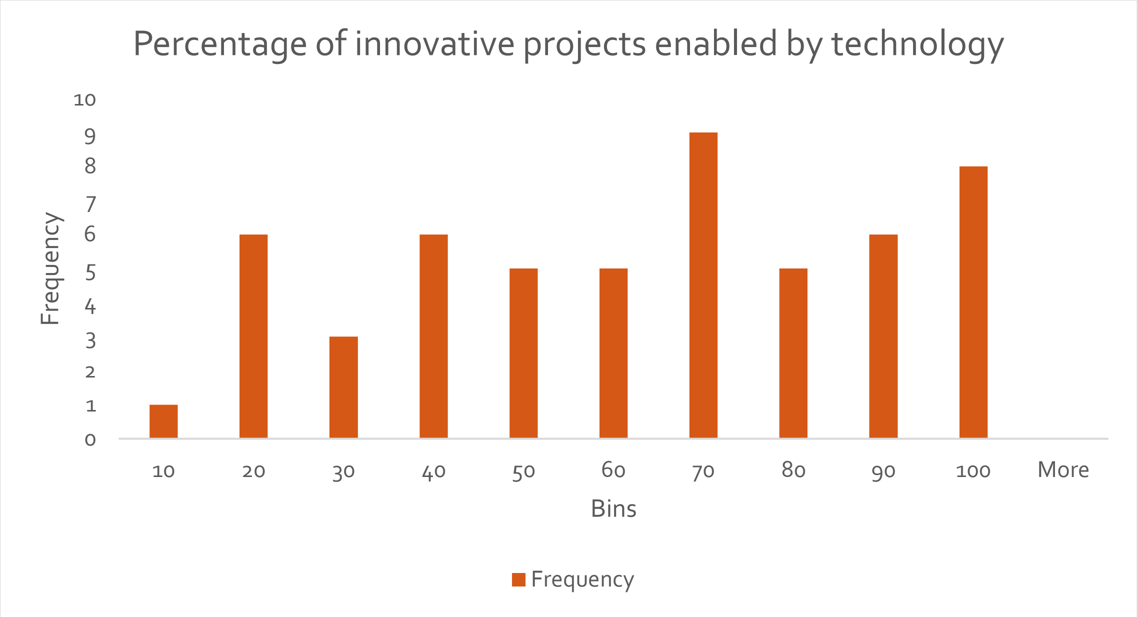


Figure 6 – Histogram: Percentage of innovative projects enabled by technology

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, one of the speakers on "The Digital Transformation of Industries" panel at the WEF 2016 conference was 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

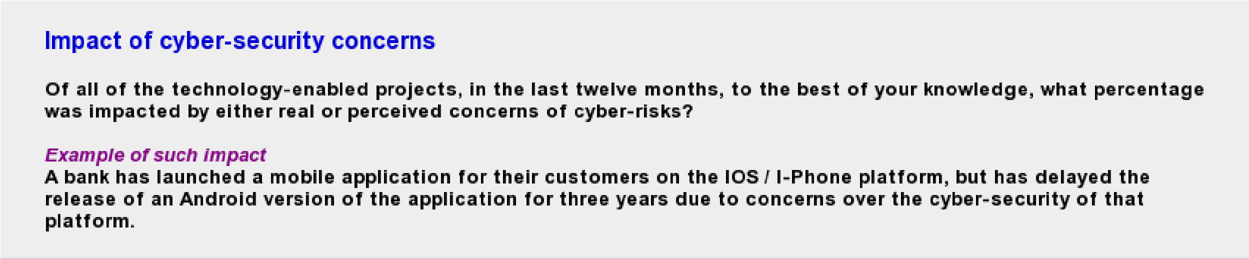
Types of impact

Next, the impact that cyber-security related activities are having on these innovative projects was examined. The impact analysis falls 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, these three questions were asked separately, and then the largest reported impact for a company was used 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, it is 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 question shown in Table 7 was posed:

Table 7 – 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.

The histograms in Figures 7, 8, and 9 visually demonstrate the spread of the responses.

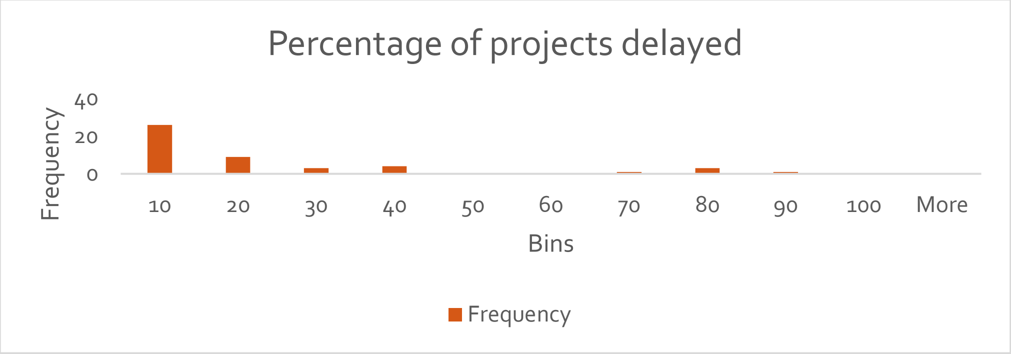


Figure 7 – Percentage of projects delayed

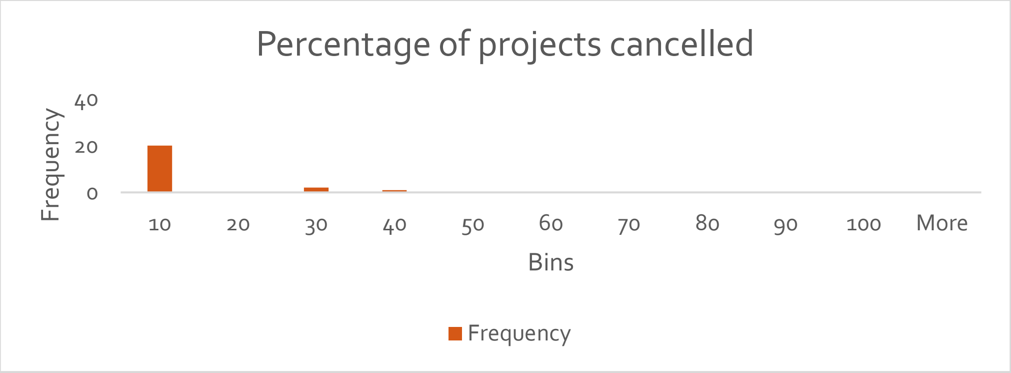


Figure 8 – Percentage of projects cancelled

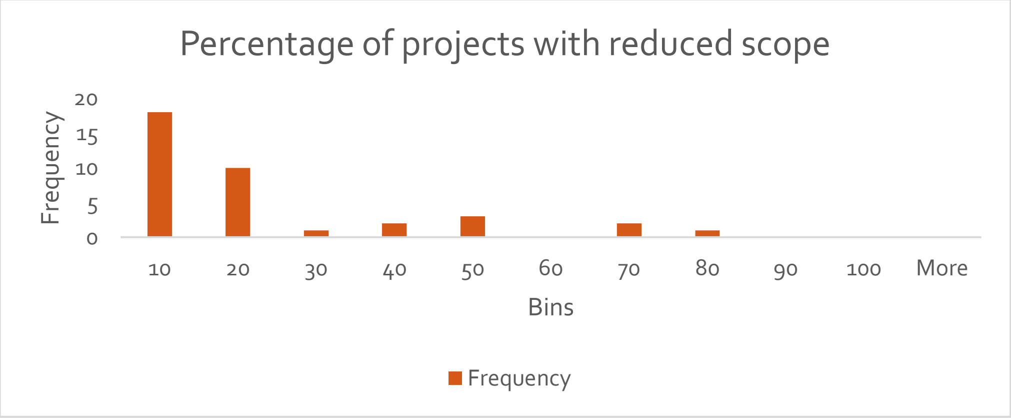


Figure 9 – Percentage of projects with reduced scope

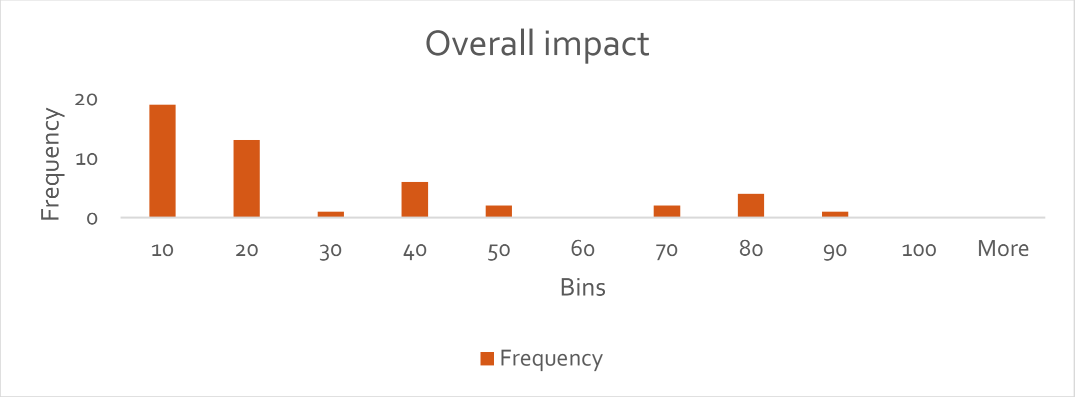


Figure 10 – Overall impact of cyber-security controls on technology-enabled innovation projects

Figure 10 summarizes 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 (320% - 50% of projects are impacted);
- A group with high impact (above 50% of projects are impacted, with 70% - 90% being the most common occurrence).

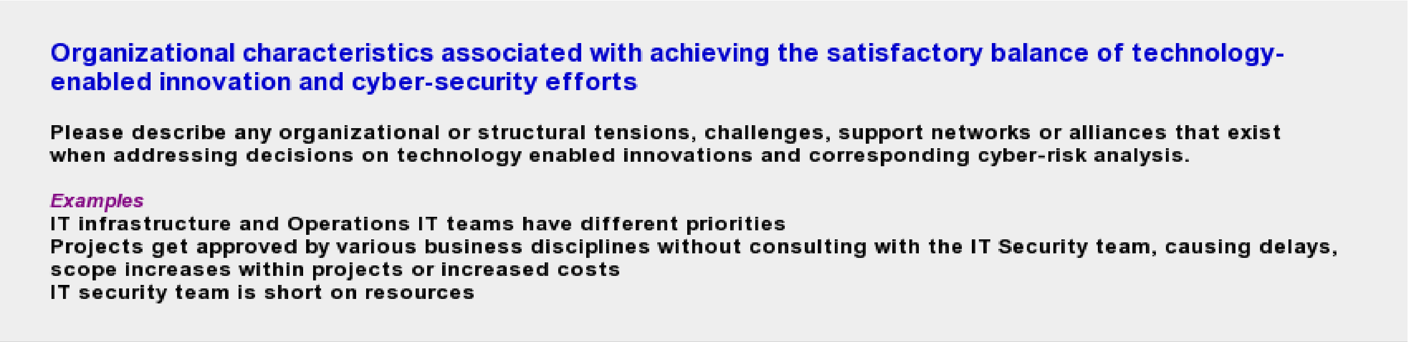
The most common types of such negative impacts are delays and scope reductions, with cancellations being a rare occurrence.

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 8. 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 9;
- **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 10; 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 11`.

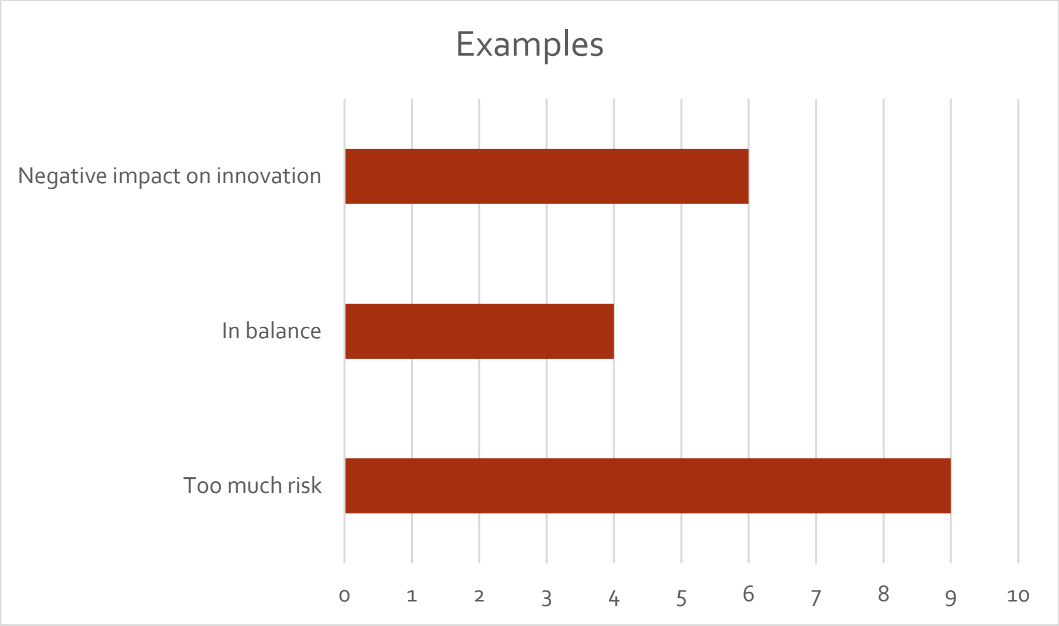
- **Table 8 – Examples of organizational issues and tensions caused by cyber-security and technology-enabled innovation**



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 discussed in the next section.

Examples of the negative impact on innovation

Table 9 – 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 10 – 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 11 – 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, it is important to see how the three dimensions were connected, utilizing the originally envisioned framework. While the data from 54 surveys cannot provide statistically accurate results, at least a pattern could be examined in more detail through the interviews. Here are the most pertinent findings.

First, number of companies in each quadrant was examined to test the original hypothesis. The results are demonstrated graphically in Figure 11:

- 27.78% of companies came in "below average" on both the "Technology Innovations" as well as "Cyber Security Maturity" measurements; the 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; the 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; the 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; the hypothesis for this quadrant was 10% - 15%.

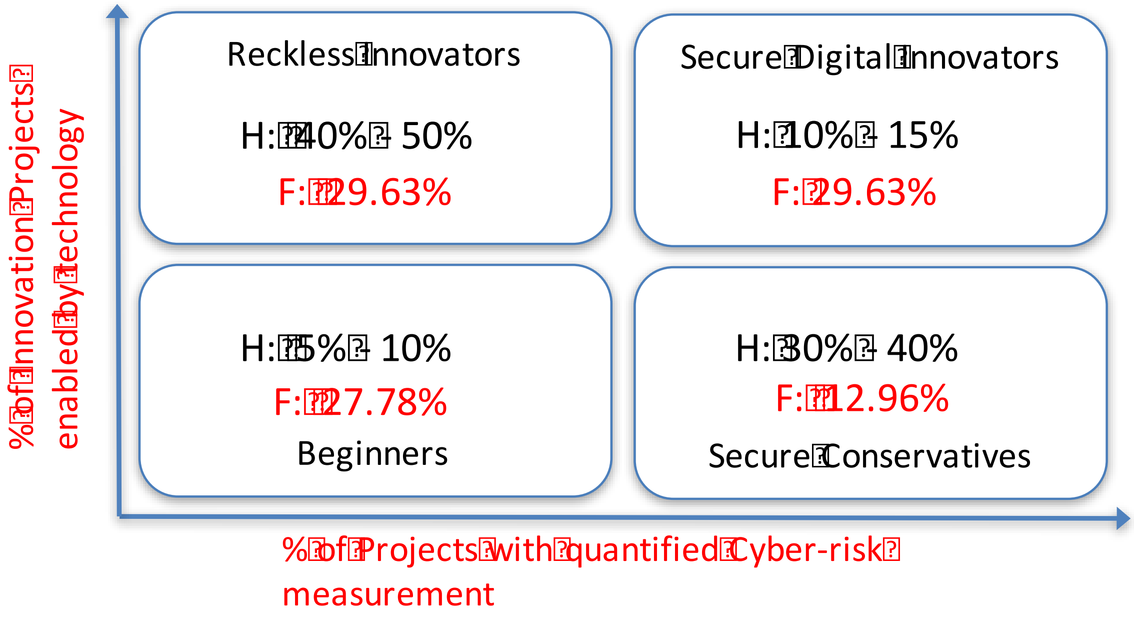


Figure 11 – Framework – comparing original hypothesis (in black) against survey data (in red)

Based on these results, the originally envisioned framework was modified 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, it is recommended that all of the labels be removed that might carry negative connotation or simply be inaccurate;
- Averages to be utilized as the dividing lines, which means that over time quadrants will shift, and companies might easily shift from one quadrant to another;
- The "size of the bubble" was added as the third dimension, to represent the negative feedback that an organization experiences due to cyber-security controls;
- A color dimension was added 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, a quadrant-by-quadrant analysis was utilized. 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 - “below average” on “Technology Innovations” and “Cyber Security Maturity”

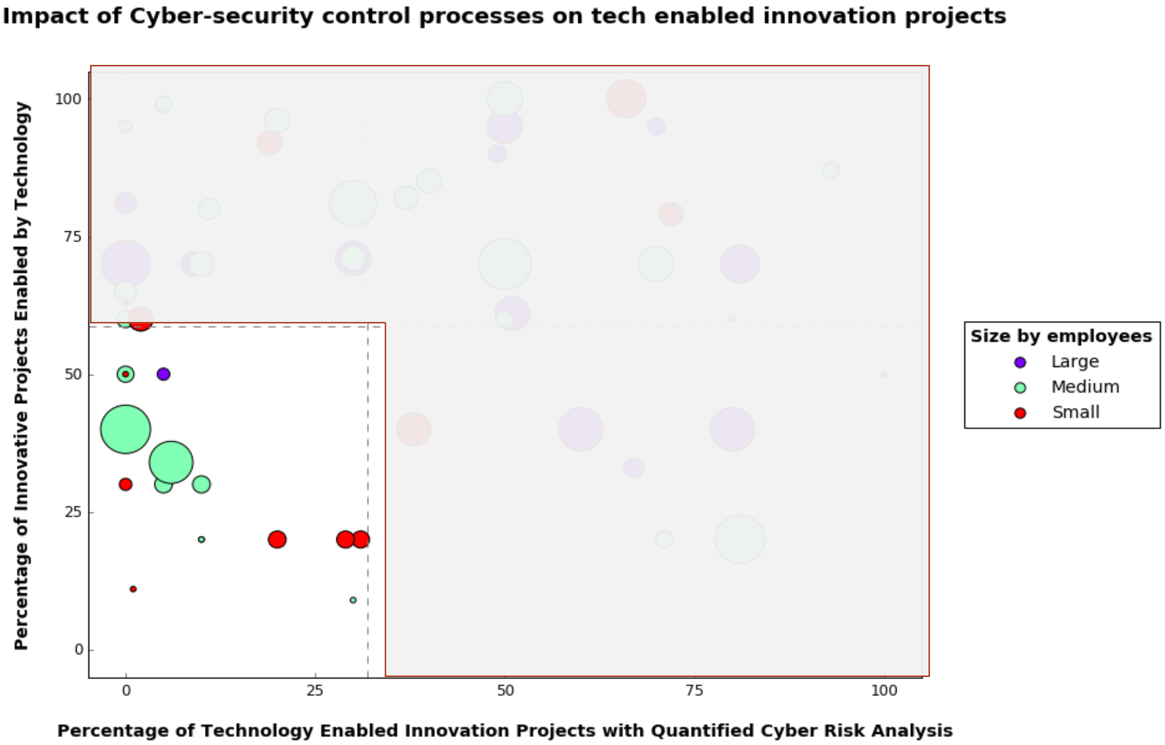


Figure 12 – 1st Quadrant: Impact of cyber-security control processes on technology enabled innovation projects

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 the 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 - "below average" on "Technology Innovations", but above average on "Cyber Security Maturity"

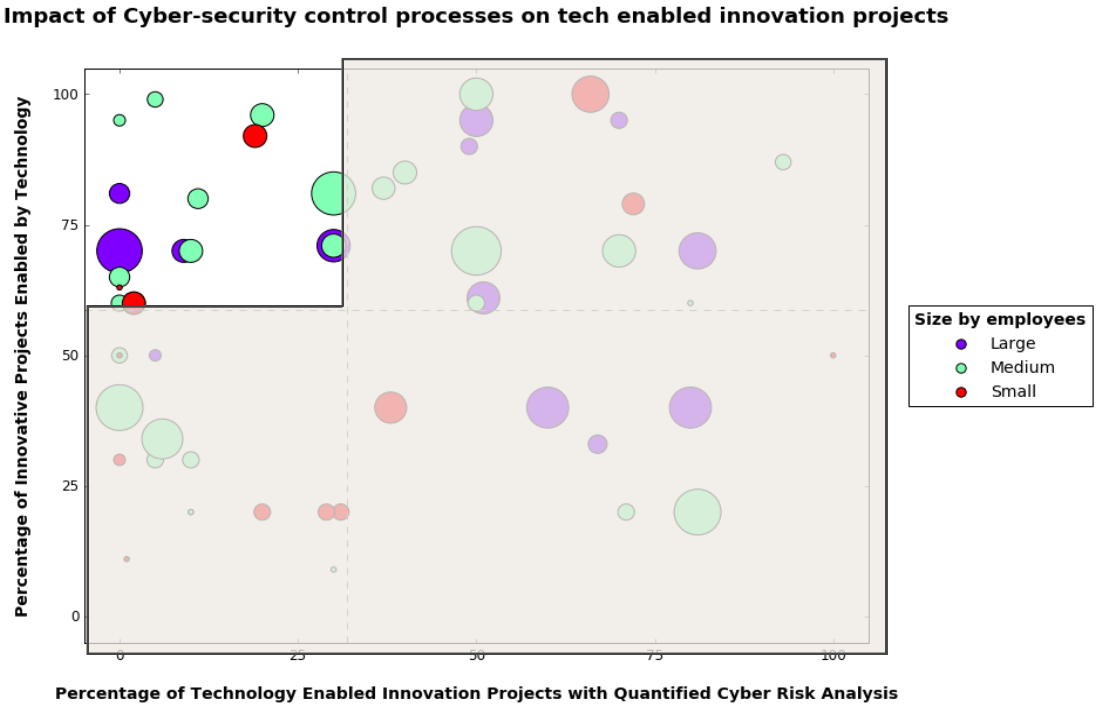


Figure 13 – 2nd Quadrant: Impact of cyber-security control processes on technology enabled

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 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 the 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 - "above average" on "Technology Innovations", but below average on "Cyber Security Maturity"

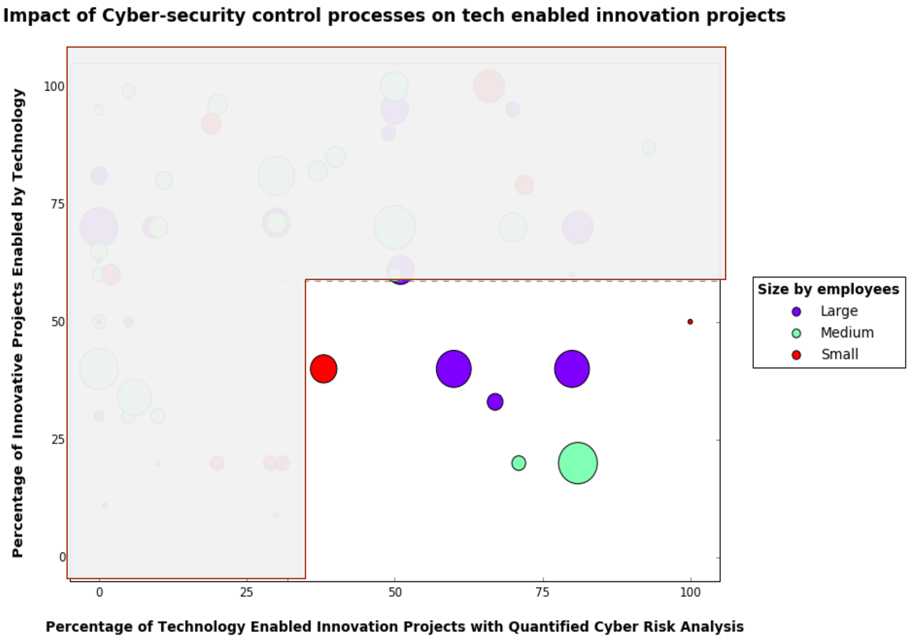


Figure 14 – 3rd Quadrant: Impact of cyber-security control processes on technology enabled innovation projects

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 the 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 - "above average" on "Technology Innovations" and on "Cyber Security Maturity"

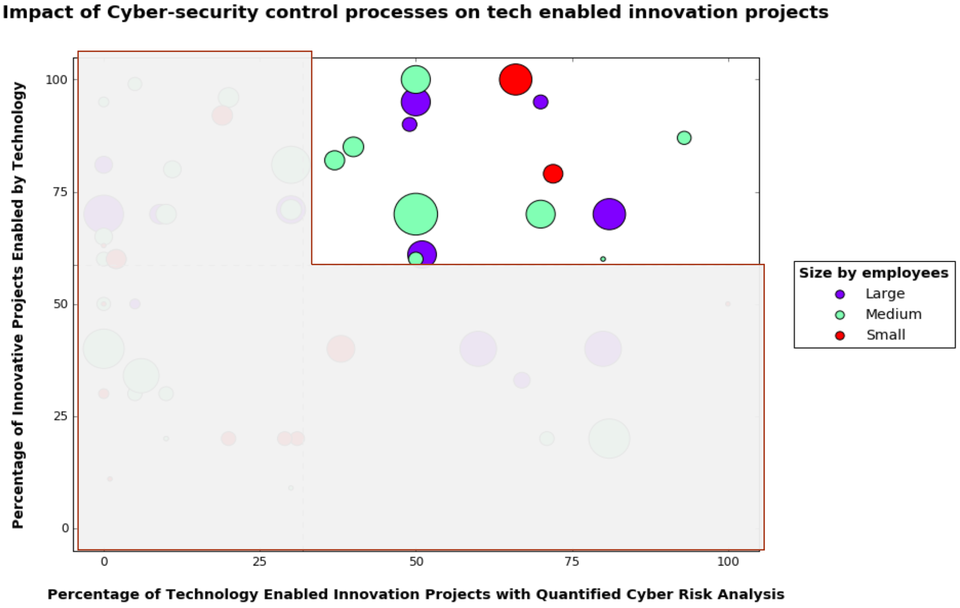


Figure 15 – 4th Quadrant: Impact of cyber-security control processes on technology enabled innovation projects

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 the 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."

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, the following simple set of steps are recommended to CIOs and CISOs, as they review these results:

- **Evaluate which quadrant the company is in,** using the same questions as were posed in the survey,, 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**.

Bibliography

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.

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

Evans, Nicholas D., et al. *The cybersecurity needs of the borderless enterprise*. Computerworld, 27 Nov. 2012. Web. 11 May 2015.

Golden, Bernard. *5 IT industry predictions for 2016 from Forrester and IDC*. CIO, 20 Nov. 2015. Web. 25 Apr. 2016.

McCandless, David. *World's biggest data breaches & hacks*. 2016. Web. 1 May 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.

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.

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.

Schwab, Klaus. *World economic forum annual meeting 2016*. World Economic Forum, 19 Apr. 2016. Web. 25 Apr. 2016.

"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.

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.