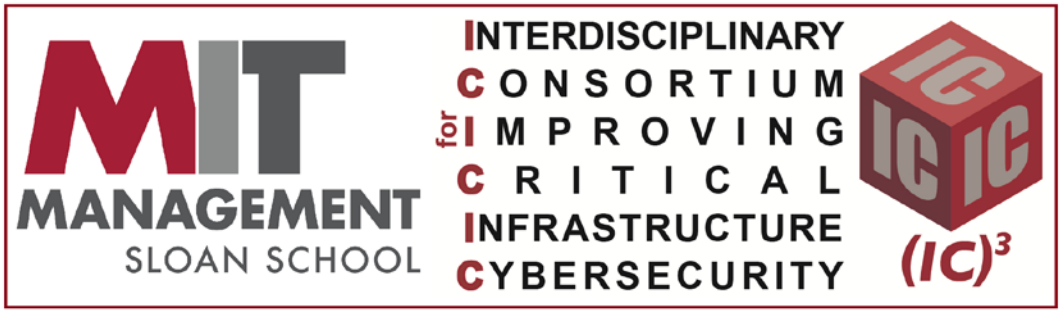

Studying the Tension Between Digital Innovation and Cybersecurity

Natasha Nelson
Stuart Madnick

Working Paper CISL# 2017-04

April 2017

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

Studying the Tension Between Digital Innovation and Cybersecurity

Completed Research Full Paper

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

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

Abstract

With increasing economic pressures and exponential growth in technological innovations, companies are increasingly relying on digital technologies for innovation and value creation. But, with increasing levels of cybersecurity breaches, the trustworthiness of many established and new technologies is of concern. Consequently, companies are aggressively increasing cybersecurity of their existing and new digital assets. Most companies have to deal with these priorities simultaneously which are frequently conflicting, and creating tensions. This paper introduces a framework for evaluating these risk/reward trade-offs. Through a survey and interviews, companies are positioned in different quadrants on an innovation/cybersecurity matrix overlaid with the negative impact of cybersecurity controls on the innovative projects. The paper analyzes the industry level, firm level, technology management, and technology maturity factors that affect these trade-offs. Finally, a set of recommendations is provided to help a company to evaluate its positioning on the matrix, understand the underlying factors, and how to better manage these trade-offs.

Keywords

Cybersecurity, digital innovation, CIOs,

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).

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?'"

Negative impact of Cybersecurity related losses

On the other hand, many CIOs continue to maintain the responsibility for the on-going management of the cybersecurity efforts. As a result, they are constantly needing to increase investments in cybersecurity 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 often report to CIOs, and are required to regularly attend the board of directors meetings with a cybersecurity 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.

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.

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, Mossack Fonseca, and Ukraine power grid also suggest new levels of sophistication and different motives for the attackers.

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 cybersecurity reviews (delays and scope reductions). The implications of increased caution and inefficiencies can in part be traced to the complexity of identifying the appropriate cybersecurity solutions for the business.

Finally, there are a series of trade-offs that companies make that may potentially lead to either direct or indirect cybersecurity related losses. Examination of these tensions is one of the key points of this research, which will be examined 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 1) that plots companies into four different quadrants as follows:

- The X axis would measure the maturity of cybersecurity within an organization;
- The Y axis would measure to what extent an organization depends on technology innovations.

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

Based on past experience and literature review of articles on a related subjects, we hypothesized that:

- 5% - 10% of the companies would be "below average" on both the "Technology Innovations" as well as "Cybersecurity 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 "Cybersecurity Maturity" measurements; called the "Secure Conservatives";
- 40% - 50% of the companies would be "above average" on the "Technology Innovations", but below average on the "Cybersecurity Maturity" measurements; called the "Reckless Innovators";
- 10% - 15% of the companies would be "above average" on both the "Technology Innovations" and on the "Cybersecurity Maturity" measurements; called the "Secure Digital Innovators".

These hypotheses are depicted in black on Figure 1.

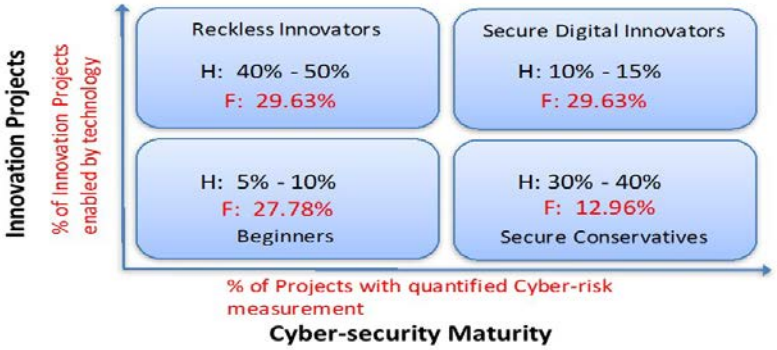

Figure 1 – Cyber Security Maturity and Innovation matrix
[comparing original hypothesis (in black) against survey data (in red)]

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 cybersecurity concerns, a survey was conducted from December 2015 to January 2016. The survey was distributed to 54 diverse organizations. 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 demographic facts about the organizations surveyed:

- Regions Asia/Pacific (21), Europe/Africa (10), Latin America (2), North America (21).
- Industries: 16 – ranging from Banking to Travel and Hospitality.
- Roles: 10 – ranging from Board Member (4), CEO (6), CISO (12), to VP of IT (4).
- Size of organization: Small - < 1,000 (13), Medium – 1,000 to 9,999 (28), Large - > 10,000 (13).

When designing the survey questions, it was necessary to address the fact that neither cybersecurity maturity nor level of technological innovations within companies were 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 focusing 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 of the survey on a question by question basis are reviewed below.

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 question asked was:

> **Measuring cyber risks:** To the best of your knowledge, in the approval process of these technology-enabled initiatives, what percentage of the included quantified risk analysis, including measuring cyber-risk?
> Examples of measurable risk analysis:
> Estimated percentage of defective parts, and associated replacement costs, number of late deliveries and associated costs.

The results of the risk-measurement question are shown in Figure 2.

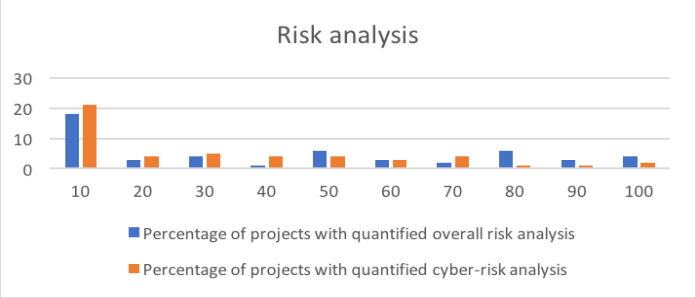

Figure 2 – Risk analysis

From Figure 2, we can see that overall risk measurement on projects is not a common practice, cyber-risk measurement in particular trails behind. Despite imperfections of the measurement methodologies, those that measure their cyber-risk activities achieved a greater degree of transparency and changed behaviors (as will be demonstrated latter). In some instances, there appears to be "too much" reporting that is too complex to understand. These reporting mechanisms are not as effective and don't generate the same positive results.

Perhaps the most critical aspect of all the 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

Examples from an interview with a CIO of a Pan-European transportation company, demonstrated both "ends of the spectrum" right from within his firm, a holding company with multiple separate companies.

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. 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 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;

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 question asked was:

> **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 organization were empowered by or enabled by technology? Value creation comes from projects that generate revenues, save costs, generate efficiencies, improve customer experience or improve product.
> Examples of value-creating technology enabled projects:
> Mobile applications, ERP, Mobile commerce, Internet of Things projects, Big Data projects.

The results of the innovation measurement question are shown in Figure 3.

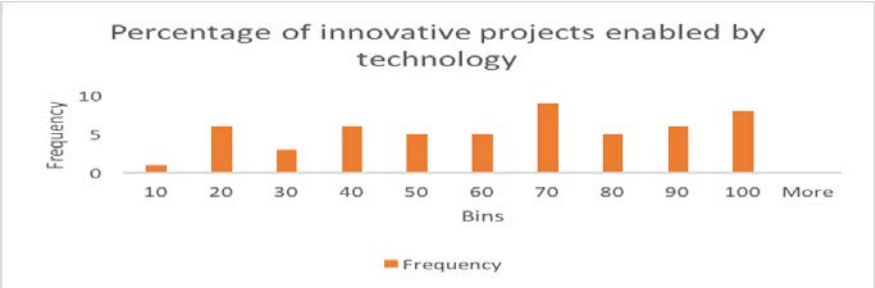

Figure 3 – Histogram: Percentage of innovative projects enabled by technology

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 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. For example, one of the speakers on "The Digital Transformation of Industries" panel was Jean-Pascal Tricoire, who is Chairman and Chief Executive Officer, Schneider Electric SA, who described the impact of digitization on energy and automation, and how his company leverages these opportunities.

> ... Now that 60% of R&D is in software, ... 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.

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 Cybersecurity control processes

Types of impact

Next, the impact that Cybersecurity 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 Cybersecurity concerns;
- Percentage of technology-enabled projects cancelled due to Cybersecurity concerns;
- Percentage of technology-enabled projects with reduced scope due to Cybersecurity 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 Cybersecurity 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, this question was posed:

Impact of cybersecurity concerns: Of all the technology-enabled projects, in the last twelve months, what percentage was impacted by either real or perceived concerns of cyber-risks?
Examples of value-creating technology enabled projects:
A bank has launched a mobile application for their customers on the IOS / iPhone platform, but has delayed the release of an Android version of the application for three years due to concerns over the cybersecurity of that platform.

The average statistics of the responses are shown in Table 1.

Table 1 – impact of Cybersecurity concerns

Impact of due to cybersecurity	
Percentage of all projects delayed	20.04
Percentage of all projects cancelled	14.19
Percentage of all projects where scope	23.98

Figure 5 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. 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.

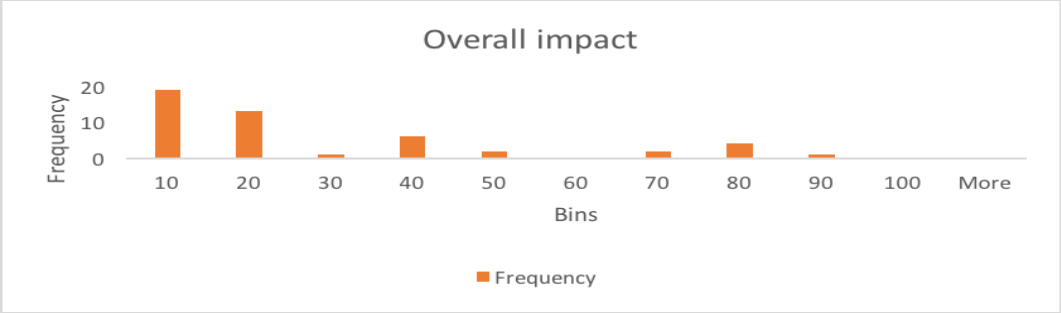

Figure 5 – Overall impact of cybersecurity on technology-enabled innovation projects

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 cybersecurity 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 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. 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:

- **6 organizations**: Negative impact on innovation: these respondents provided examples where strong cybersecurity came at the expense of innovation, creating tensions and perceptions of reduced value;
- **4 organizations**: In balance: these respondents provided examples where innovation and cybersecurity efforts were well balanced;
- **9 organizations**: Too much risk: these respondents felt that the company was taking on too much risk in order to achieve their innovation objectives, thus creating tension.

Some examples provided below.

Example 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."

Example of a well balanced approach: "We reduced (contained) the scope of data in our BI toolset specifically to ensure that data is not inadvertently leaked while doing analysis."

Example of too much risk: "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."

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

Finally, and most importantly, it is possible to see how the three dimensions were connected, utilizing the originally envisioned framework on Figure 1. While the data from 54 surveys cannot provide statistically validated 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 1 in red:

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

Based on these results, the originally envisioned framework was modified in the following ways and depicted in Figure 6:

- 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 moved 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 Cybersecurity controls;
- A color dimension was added to 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 cybersecurity within an organization;
- The Y axis measures to what extent an organization depends on technologies to execute their value creating innovation agenda.

1st Quadrant: Impact of Cybersecurity control processes on technology enabled innovation projects

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 cybersecurity controls.

Why would companies find themselves in this quadrant?

- Many start-ups are just building 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. One might assume that the start-ups will have a high percentage of innovative projects, but 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 are marketing, financial, and operational. As the company grows and product develops, things will change, they can start taking on more innovative 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.

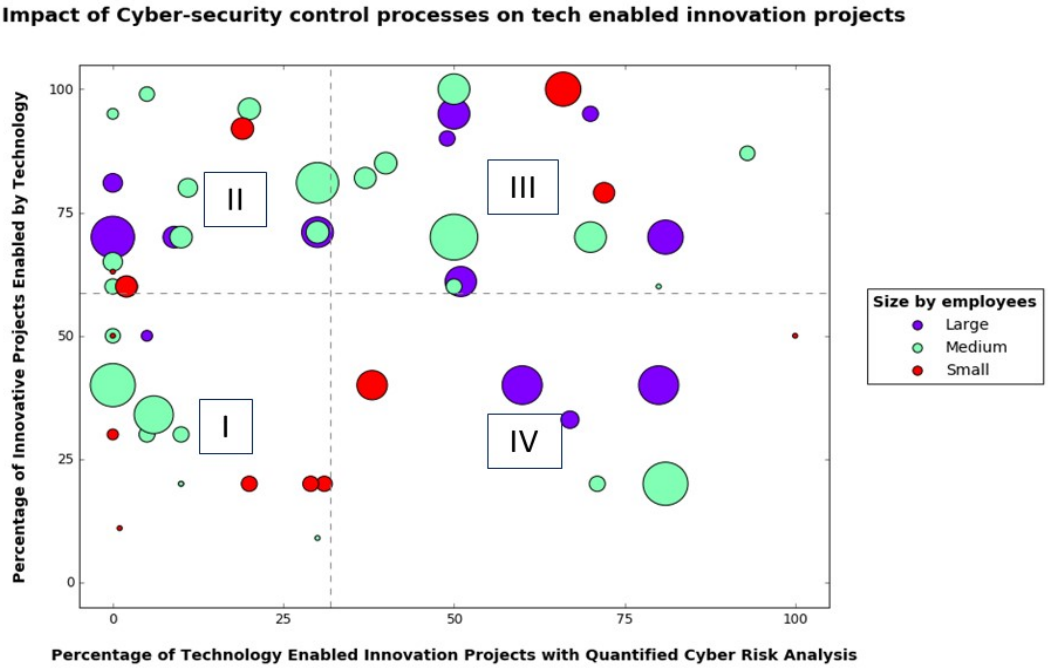

Figure 6. Results of Individual Companies

[The "size of the bubble" represents amount of the negative impact that an organization experiences due to cybersecurity controls, in this figure; the color dimension indicates size of the company]

2nd Quadrant: Impact of Cybersecurity control processes on technology enabled

In this 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.
- Companies with high competitive pressures to innovate are either in this or 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, for reasons described later, risk is not being properly addressed.

3rd Quadrant: Impact of Cybersecurity control processes on technology enabled innovation projects

In this 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, but has the least number of companies (13%). Negative impact is split – three companies have large negative impact, three companies have low negative impact and one is in the middle. Companies in this quadrant may lose out on the opportunities to achieve competitive advantage through technology: 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 industries where competitive pressures are not as high, 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.

4th Quadrant: Impact of Cybersecurity control processes on technology enabled innovation projects

This quadrant consists primarily of medium and large firms, plus two small firms. 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 there are companies that experience high negative impact from cybersecurity 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 or second quadrant;
- All of these companies noted the necessity to mitigate cyber-risk as they build digital capabilities.

Conclusions and Recommendations

The rapid pace of technological innovation is continuing to offer companies an unprecedented number of new value creation opportunities. In parallel, cybersecurity 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.

According to our findings, only 13% of companies believe that they have found the right balance between the two priorities. 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.

The following factors may impact which Quadrant a company falls into:

Industry related factors: cybersecurity 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 cybersecurity posture and related strategy.

Company factors and technology management practices: are those that companies have most control over. From this study, however, these factors have the highest numbers of issues, specifically:

- Operating model and organization structure;
- Company culture and tensions created by cybersecurity efforts;
- Board of directors and their role in cybersecurity and innovation trade-off decisions;
- Education, communication and organizational awareness;
- Legacy architectures;

- IT governance and resource allocation.

Maturity of technologies: considered for various innovation projects also plays a significant role in the amount of cyber-risk and how it gets addressed.

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 cybersecurity gets built into all new innovative technologies at the foundational levels.

Practical recommendations: the following steps are recommended to CIOs and CISOs:

- Using the same questions, evaluate which quadrant the company is in.
- Adjust for the industry factors and the company's inherent risk posture to see which quadrant would be most appropriate in the short and long run. If there is no current cybersecurity regulation or it is not enforced, the company may be exposed to a weaker security posture.
- Evaluate board and senior leadership support; use frequency, length and interactivity of the board cybersecurity briefings as a proxy to compare against others in this study.
- Examine cyber-risk measurement practices; specifically, whether the risk is measured, how often it's measured, its uses in 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.
- Check for the culture, education and awareness at all levels and strong technology management and governance practices.

REFERENCES

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

"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.

Nelson, Natasha, *How companies achieve balance between technology enabled innovation and cyber-security*, Thesis: M.B.A., Massachusetts Institute of Technology, Sloan School of Management, 2016.

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

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.