Identifying How Firms Manage Cybersecurity Investment*

Tyler Moore Scott Dynes Frederick R. Chang
Darwin Deason Institute for Cyber Security
Southern Methodist University
Dallas, TX, USA
deasoninstitute@smu.edu

October 28, 2015

1 Study Overview

A few years ago most firms would manage cybersecurity and make investment decisions based mainly on industry best practices, resulting in their adopting certain technologies, policies and practices, without a detailed understanding of their specific overall cyber risk situation. As a result, very few successfully developed and deployed a strategic, comprehensive and effective cyber risk management framework. Lacking a clear articulation of how cyber risks integrate into organizational risk, many firms experienced a persistent under-funding of information security budgets.

Over the past couple of years the landscape has changed dramatically. Cyber risk is now a board-level concern, and everyone is sensitive to cybersecurity. Has this heightened awareness changed how firms now prioritize their (still-limited) security budgets? Are return-on-investment (ROI) models being used, which would indicate a greatly matured approach to cyber risk management? Are other frameworks being developed to address the growing perception that many of the most damaging cyber risks may not be accurately characterized by ROI models, which struggle to deal with broader concerns such as reputational damage? How are firms actually managing cyber risks and deciding how to make substantial investments? What are the key motivations driving cybersecurity investments: cost-reduction, regulatory compliance, risk reduction, process improvement, and/or something else?

This is a report on a set of semi-structured interviews with information security executives and managers at a variety of firms. Section 2 details the methodology, and the subsequent sections present the key findings. Section 3 describes how organizations are supported in terms of budget and by senior management, along with how that has changed. Section 4 examines how cybersecurity investment decisions are made, including how organizations prioritize, using metrics and especially frameworks. Section 5 examines the suitability of information decision makers have in managing risk and selecting vendors for security controls. Section 6 compares findings across different sectors, while Section 7 examines the unique circumstances facing government CISOs. Section 8 discusses three cases of "CISO Mavericks" whose approach differs significantly from the rest. Finally, we conclude in Section 9.

2 Methodology

2.1 Survey population

We recruited a total of 40 executives for this study; the great majority of the interviewees were CISOs, with a handful of CIOs and other roles. We selected participants primarily from large firms across four industries: healthcare (5 firms), financial (8), retail (8) and government (11). The remainder came from other sectors, such as energy, automotive and higher education. 31 participants came from US organizations, with the remainder international.

Participants were recruited by a variety of means. IBM identified the majority of participants, passing along contact information for us to reach out directly.

2.2 Semi-structured interview approach

We carried out the interviews using a semi-structured approach. We aimed to cover each of the study questions in every interview; these questions would serve as a launching point for follow-on questions in a conversation with the subjects.

Interviews were conducted either in person or via phone with one or two researchers[1]. Interviews lasted from 30 minutes to 1 hour. At the start of each interview we asked interviewees to sign a consent form, which made clear that the interview was confidential, that any results from the interview would be presented in an anonymous fashion, not mentioning the interviewee or their firm, and that the interviewee could choose to not answer any question or terminate the interview at any time. During the interview, efforts were made to build a

[1]The research methodology has been reviewed and approved by SMU's human subjects division as IRB 2014-130-MOOT.

high degree of trust with the interviewee(s), based in part on the interviewers' and subject's shared expertise in cybersecurity.

Questions were broken down into three broad categories: grounding questions, macro-level, and micro-level questions. The grounding questions were designed to elicit information about the subject's background and role within the organization. Macro-level questions focused on how threats were identified, managed and prioritized in general. We also inquired about the degree of support from management, how that has changed, and the use of metrics in guiding investment decisions. Micro-level questions focused on the experience of a recent large cybersecurity investment project. We asked about the decision-making process, their satisfaction with available information, and any link to the metrics used in prioritizing threats. The full list of questions is given in the Appendix.

The advantage of a semi-structured interview methodology is that it enables the researchers to glean detailed contextual information that would not be possible using a structured survey instrument. It does not presuppose what the answers to questions should be, which enables us to uncover new and unexpected findings. It also enables us to get a deep understanding of how each interview subject approaches the highly complex challenge of securing a large organization.

The disadvantage of the semi-structured interview methodology is that the contextual findings we report do not generalize to the profession as a whole. Even though we interviewed a large number of executives across many sectors, the unstructured portions of the interviews were so personalized that our findings must be interpreted as exploratory in nature.

On balance, we believe the semi-structured interview approach is the most appropriate instrument for studying these complex issues. We hope that many of the findings we report can be corroborated with other methods, such as by carrying out more structured interview questions informed by the preliminary findings given here.

Note that the respondent opinions presented here do not necessarily reflect the opinions of the study authors or the study sponsor, IBM. Our objective is to relay as accurately as possible the statements of the interview subjects.

3 Organizational Support for Cybersecurity

3.1 Support from upper-level management

Broadly, senior-level management and company boards are supportive or very supportive of cybersecurity efforts. 81% of subjects reported that their upper-level management is supportive of their activities. 85% reported that the level of support has been increasing,

with the remainder saying that support has remained unchanged. No one said that the amount of support they are receiving with respect to cybersecurity is decreasing.

When asked why there was such a high level of support, most interviewees mentioned recent breaches that have been heavily covered in the news – the Anthem breach was brought up many times, as it was the latest breach in the news when most of the interviews were conducted. While breaches have sensitized senior management to the need for improved cybersecurity in the past, the recent breaches have for some reason been attributed as a tipping point for high-level support from the great majority of non-government firms interviewed.

One CISO characterized the situation as there being a "hunger for security in the company". His[2] "senior management has gotten religion about how important security is". He contrasted this with how things were only a few years ago.

As will be detailed later in this report, cyber risk is becoming or has become a first-class risk, and funding for cybersecurity projects reflects this. Most CISOs say that getting budget for their projects is not a challenge; in a few cases CISOs said that senior management would like them to do more. Where CISOs did get push-back on their budget requests, the reason was often that senior management was concerned that the CISO's organization would not be able to execute on the volume of proposed projects, not that they objected to the projects themselves. This is reflected by the observation that 40% of participants reported receiving some push-back from management.

There were a few exceptions: five subjects reported that they did not feel they received adequate support from senior management. For example, the CISO at a large European retailer reported that the board is not supportive of cyber programs. These firms had not experienced problems resulting from a lack of cybersecurity in the recent past (which is different than saying they were secure), and as a result saw no need to go above what was required from a regulatory compliance perspective.

At the board level it was common for the CISO to directly or through their reporting chain report out on the cybersecurity stance of the firm. Some boards had cyber-specific subcommittees that the CISO was a member of. One CISO who reports to the CIO notes that "the [IT security advisory] board helps provide that layer of oversight and the opportunity to have senior-level visibility that I might not otherwise have".

3.2 How have budgets changed over time, and why?

Outside of government, cybersecurity budgets have generally been growing. 88% of participants report that their security budget has increased, with the remainder saying it has

[2]We use male pronouns throughout to refer to interview subjects regardless of gender, in order to protect the anonymity of participants.

remained the same. (For a discussion of the impact of budget on government CISOs, see Section 7). The level of attention cybersecurity has received in the press and as a result of breaches has created an environment where most firms are prepared to make substantial investments. In the words of one CISO whose budget has nearly doubled, "Honestly, I have not seen a case where I asked for money and it's been turned down. It's a unique time in the field because of the hype."

How are CISOs effectively making the case for more budget? A common refrain was the use of frameworks. In the words of one CISO, "Security has to be able to have a basis to argue its point of view in a compelling story with some thought behind it, rather than 'I want to get these things because it's the next cool security thing that's out there'." Senior leadership is "looking for me to articulate what the security strategy is in words, in projects, and in dollars that make sense to them", and the framework facilitates that. A retail CISO says that frameworks help him clearly articulate the key message when making new investments: how risk levels change, the spend required to execute, and how to prioritize. It makes for a far easier conversation than were he to say he needs a collection of solutions to reduce risk within the environment because the solutions all sound the same all the time to senior leaders.

According to a CISO for a large retailer who has suffered a high-profile breach, senior management was prepared to invest substantially in security following the incident. But they wanted to do so in a thoughtful and measured way. The current CISO was recruited to the company to bring "planning and science into where to spend", as well as offer guidance on how quickly they can ramp up capabilities without taking on more than can be managed. A custom framework built on ISO and NIST guidelines has satisfied management that the CISO has a solid plan for investment. More detail on the use of frameworks is given in Section 4.4.

Another tried-and-true way to win budget is to point to compliance obligations. While compliance does drive a significant portion of security investment, the most effective CISOs tended to avoid making cases based primarily on compliance alone. As one CISO remarked, "I try, in everything that I communicate about why we're investing in security, I always try to make the compliance argument the last thing because I think that way too many programs are aligned around 'What's the minimum thing I have to do to get a check mark? And if I get a check mark I must be fine'. I don't really talk about the security program from a compliance standpoint very often." It is worth noting that this CISO has leveraged frameworks to win a greatly increased budget. By contrast, three of the four subjects who stated that upper management does not support their cybersecurity efforts also reported that compliance arguments were the main way they could win more budget.

Another approach effective CISOs take to get buy-in is to engage business units by understanding their risks and making security 'real' for them at their level. One government CISO looks for internal infosec "champions" and engages them directly. Another government CISO would demonstrate the vulnerabilities to the CIO or the business owners. Business owners were preferred, as they had the power to harp on the CIO to make changes happen.

3.3 Perceptions of adequate spending levels

One of the structured questions we asked was whether the interviewees felt that they and their peers were spending too little/ about right / too much on cybersecurity. Slightly more than half said that they were spending too little; this did not meaningfully vary by sector. One factor that did have a slight correlation was the use of a framework. All the firms that felt they were spending appropriately had a framework (10 firms). Of the firms that felt they were spending too little, 2/3 utilized a framework and the remaining 1/3 did not (12 firms total).

As will be presented below, CISOs found that their using frameworks aided their efforts to develop an understanding in senior leadership of the business consequences of insufficient cybersecurity. It is not clear if this is the reason these CISOs felt their firm was investing too little; but it does seem that strongly embracing frameworks is associated with the belief that firms are investing sufficiently.

One intriguing finding was that although 46% of subjects believe that their organization was spending about the right amount on security, only 7% believed that their peers were. 64% responded that their peers were spending too little. Strikingly, 29% claimed that their peers were spending budget in the wrong areas, even though this wasn't offered as an explicit choice.

3.4 People are the primary limiting factor in budget requests

One of the surprising findings that emerged early was that budget was clearly available for cybersecurity projects. CISOs would talk about their plans, which often included increasing headcount. Some CISOs were talking about more than doubling the size of their group in the coming year.

For several firms interviewed their proposed budget got push-back — not because of the size of the budget but because senior management had concerns about the ability of the cybersecurity organization to absorb a larger budget in terms of execution and increased headcount. Internally there was agreement to and support for a particular cybersecurity project plan, but the execution concerns resulted in efforts not being funded.

CISOs from many sectors talked about the difficulty in finding and hiring skilled, talented cybersecurity personnel, despite their large professional networks. One CISO has had three slots open for months and only recently has found two suitable candidates. Another talked about how his location is not a draw, and he is recruiting from the local university. A CISO who is also recruiting from his local university acknowledged that students straight out of school know very little about the space, but says 'We all have to start somewhere'. He talked about growing the needed competencies internally, and seems resigned but confident. Yet another CISO talked about how he cannot compete with the salaries being offered. He thought he was going to hire a candidate, but could not meet the $30k higher offer the candidate had elsewhere.

As noted elsewhere (Section 7), government entities face steep budgetary constraints; for them people are not the limiting factor. Even so, they too struggle to hire, and to train those they hire. One government CISO talked about how the cap on training budget was $3k per person, per year. He was saying that's about the cost of a 4-day SANS course, and he feels his staff needs to attend multiple SANS courses a year to stay current."That's why we rely on contractors heavily", he says. Other firms rely on contractors to provide particular areas of expertise and augment their staff during projects; in some cases there's an explicit desire for these contractors to train the internal staff to use new technologies – to act in a mentoring role.

4 How are Cybersecurity Investment Decisions Made?

4.1 What are the biggest drivers of cybersecurity investment?

At the end of our interviews, we gave subjects a list of possible drivers of security investment and asked to rank their top three. The results are given in Figure 1. By far, the most frequent responses were "perceived risk reduction" and "compliance". Subjects reported that compliance obligations drive a significant fraction of the overall budget (in terms of financial outlay and employee time). Even so, there was a universal recognition that compliance can only address some of the challenges they face, at best. "Good compliance does not equal good security", as one CISO put it.

Several subjects explained that invoking compliance was the most reliable way to get projects funded. However, due to the disconnect between compliance efforts and security, other strategies were needed to support important efforts not mandated by compliance regimes.

The fact that "perceived risk reduction" was selected most often is an encouraging,

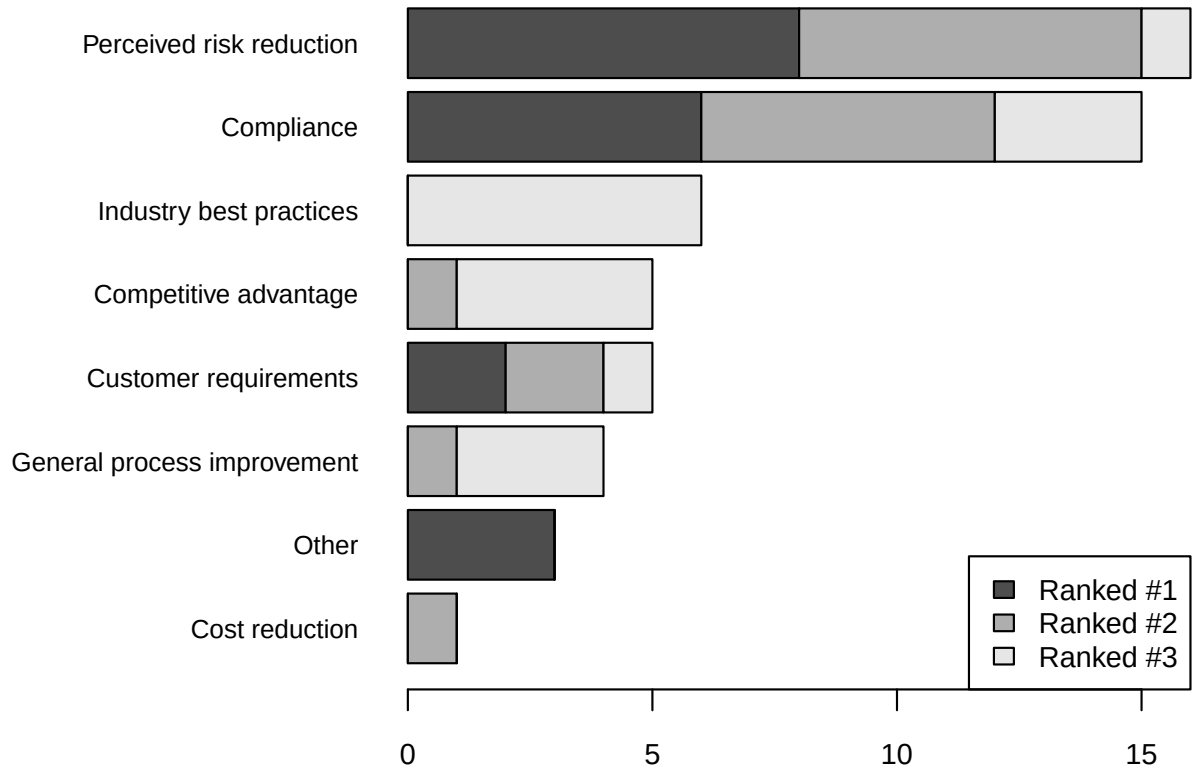

Figure 1: Responses to the question: "Please number your top 3 drivers of information security investment".

albeit unsurprising, result. CISOs are investing in security controls that, in their eyes at least, reduce the risk facing the firm. Below, we explore in greater detail how the subjects determine that the countermeasures will reduce risk, be it through using frameworks, metrics, or gut.

It is also worth noting what is not driving security investment. Cost reduction was only selected as a top driver by one respondent. Even though security is often portrayed as a cost center to the business, few CISOs view security spending as an opportunity to reduce costs for the firm. Customer requirements, while selected by a few respondents, is also not widely seen as a driver of security investment.

4.2 How do organizations identify which threats are most important and prioritize accordingly?

At the end of the interview, subjects were also offered a list of prioritization approaches and asked them to rank the top three approaches they used. Figure 2 plots the results.

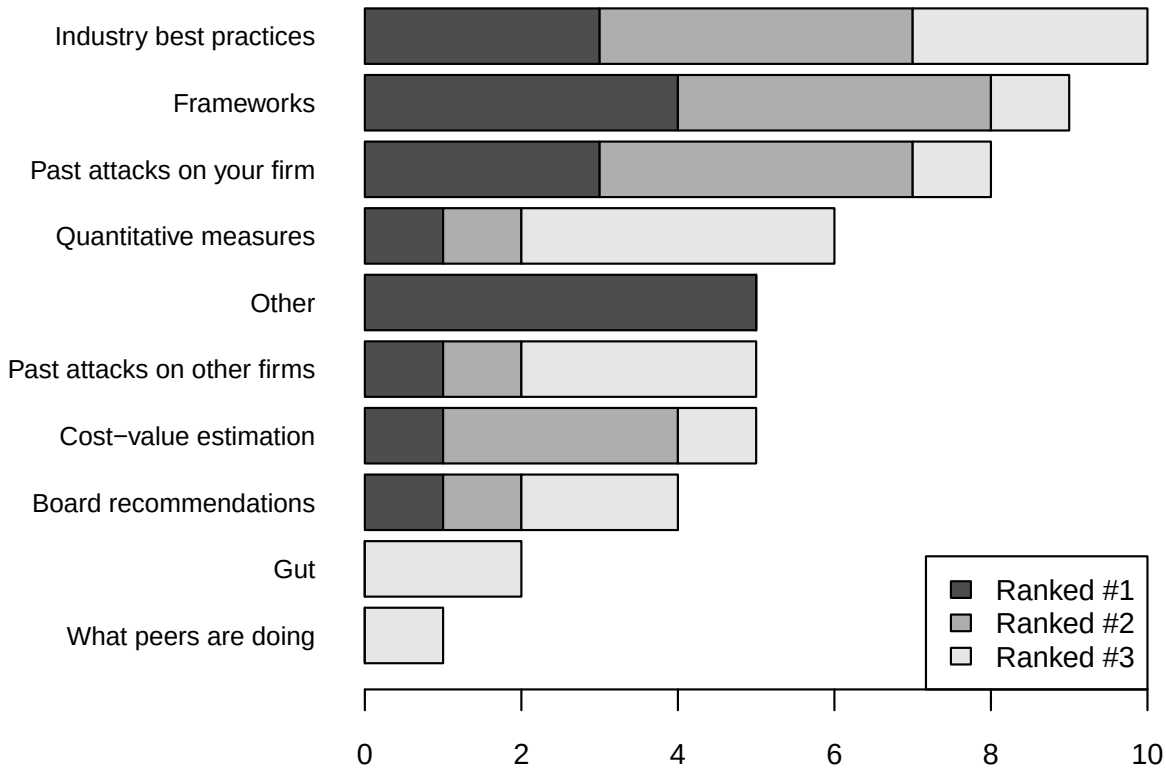

Figure 2: Responses to the question: "Please number your top 3 prioritization approaches".

It is worth noting that there was much greater variation in the responses to this question than to the question about drivers. The top two selections were industry best practices and frameworks. In fact, the exact language used for the "frameworks" response is "NIST or other formal IT-to-business risk mapping process". Based upon the interviews themselves, most of those respondents selecting industry best practices explained in the interview that they relied on a simpler framework to prioritize such as the SANS Top 20 Critical Controls. We dive deeper into the discussion of frameworks later in this section.

"Past attacks on your firm" came in third, with a substantial but lesser showing for "past attacks on other firms". In conversation, respondents selecting these responses pointed to the importance of information on incidents revealed by SIEMs and other threat intelligence. Additionally, subjects selected these responses whenever the subject or a close competitor experienced a data breach or other high-profile attack.

"Quantitative measures (e.g., ROI, NPV)" came in fourth, though notably most subjects selecting this response ranked it as only the third most important factor. We next discuss the importance of these measures to subjects, along with cost-value estimation.

4.3 Do organizations calculate ROI to make investment decisions?

The use of true quantitative metrics to guide investment decisions has been very rare. Only a few subjects have mentioned using a numeric ROI-type metric as a way of prioritizing investments. Most use of metrics have been focused on measuring and improving operational security: counting the number of unpatched machines in an organization, malware infections caught, employees falling for company-transmitted phishing emails, and so on.

A minority of subjects reported that they were still asked to place budget requests in ROI terms. This requirement was more prevalent in the financial sector. But even in cases where ROI was still used, the impression given by the respondents is that their boards are not driving its decision-making in this way.

We observed disagreement over whether or not ROI is a useful or meaningful measure to calculate. When asked if he ever made ROI calculations, one CISO replied that he and the CIO have "steered clear of FUD" (fear, uncertainty and doubt). When asked to elaborate, he stated that he does not want to sell security to the board by saying "there's a 20% chance of a $20 million breach in a given 5 years". He just doesn't think that argument resonates at the executive level.

A healthcare CISO stated that "in security, ROI is a fallacy. We are a cost center". His view is that security is a necessary business expense, and the attempt to frame spending as creating business value is doomed to fail. Some CISOs take a more nuanced view, that in certain situations, calculating ROI is feasible, even helpful, while in other cases it is not an appropriate measure. A retail CISO argued that he could plausibly assign a value to at-risk credit-card records and personally-identifiable information (PII) in order to identify securing which would lead to a better ROI. His firm holds around tens of thousands of credit-card records, whose exposure could trigger a $2 million fine, plus the cost of breach remediation. By contrast, his firm holds hundreds of thousands of records with PII. Consequently, he treats the loss of PII as a top threat, and can devise ROI measures to back that up. This same CISO noted that while calculating ROI makes sense here, in other areas such as the deployment of encryption mechanisms, calculating ROI does not make sense. He justifies countering these other threats by risk mitigation rather than frame it in terms of ROI.

Another CISO from the financial sector recognizes the difficulty of making ROI calculations, and he uses a framework that does not rely on ROI, but nonetheless he still holds it up as an ideal. He recounted one recent example that was the first time he's seen a security ROI argument that in his view could sell at a business level. The example involved software security code review. He ran a testing program over 9 months and concluded that by detecting code deficiencies early he is actually saving the org $1–2 million. He expressed hope that his organization might find similar justifications for future investments.

All this discussion about the limitations of calculating ROI should not obscure the point that metrics can be very useful as a communication tool, to both operation teams working for the CISO and to senior decision makers above the CISO. One government CISO recounted how a colleague had used metrics to incent better behavior. The colleague assembled a report card of the organization's information security posture using 20 metrics (e.g., patch times). After presenting the report cards at meetings with executives, he watched as divisions started competing to get better "grades" than others. Another CISO relied on metrics tracking risk over time to justify his spend – both the need to increase spending and the evidence of the spend's impact. He argued that longitudinal metrics can be very powerful in building a business case to senior management that security investment has been worthwhile.

While we have not seen widespread use of ROI calculations in deciding how to invest in infosec, many CISOs do think about risk in qualitative terms in a way that guides investment decisions. They are acutely aware of the many security risks reported by the media and in trade reports, and they take individual decisions about which threats are most significant to their firm. For some firms the biggest threat is data breach, whereas for others it is threats to availability. Regardless of which threats are the top priority, the CISOs focus their efforts and budgets on selecting the best countermeasures to mitigate the top risks. That the calculus lacks the precision used by traditional ROI calculations could actually be interpreted as a sign of growing sophistication: The old ROI calculations required fudging numbers in a way that might placate management but did not actually help guide the CISO's decision-making process.

4.4 The role of frameworks

Frameworks have become a very common feature of cybersecurity efforts. Frameworks are utilized for purposes ranging from compliance through highly-tailored risk assessment, prioritization, and communication/project management tools. The types of frameworks used is also broad. Many firms utilize well-known and defined frameworks such as NIST, ISO 27000, and COBIT; others develop approaches based either on these frameworks or on their own approaches and call them 'frameworks'. These extended and 'roll-your-own' frameworks often allow for the categorization and prioritization of risk in addition to mitigation using controls. For the purposes of this report we will take a broad view of what constitutes a framework.

The use of frameworks The use of frameworks does not seem to be sector-specific, with the exception of the government sector. In the US government the NIST framework plays a central role in developing controls to manage cyber risk. Adherence to the NIST guidelines

is required by the Federal Information Security Management Act of 2002 (FISMA); the resulting controls form the basis of annual audits. As a result, government entities tend to view the use of frameworks as a compliance activity. For example, one government CISO spoke about the NIST framework and his desire to keep as compliant as possible, and findings during the audits as low as possible. This CISO also had the goal of becoming secure, and not just compliant.

Not all government agencies feel bound by NIST; some see it as a bar that needs to be met. One government CISO spoke about developing a 'risk register' that went well beyond NIST; their framework for prioritizing cybersecurity investments included input from government intelligence agencies, and a separate framework used to assign a risk score to core assets. Another created a matrix that looked at 40 different areas and used this to assess security posture and maturity. This matrix was based on NIST and ISO 27001.

Frameworks are used to assess security posture and maturity, identify gaps, and prioritize available investments. Most of the interviewees spoke of having a considered, persistent way of assessing their risks (what we are defining as a framework for this report; most were not NIST/ISO/etc.); these frameworks were then utilized to characterize their risks. As most of the frameworks enabled them to rank order the resulting risks it also enabled them to establish a prioritization as well.

At least one firm used the resulting prioritization to validate the framework's veracity. One astute CISO observed that his organization would often ignore the top ten risks identified by the framework and instead focus on the 11th, because the 11th-highest risk according to the framework was actually the most important one in the eyes of his team. Afterwards, he wondered why they were investing substantial effort in using a complex framework if they were only loosely following its results? This dissonance between the framework and their perception of risk has led them to consider a simpler framework that better aligns with their expectations. We note this example raises the very interesting issue of whether frameworks are used to define or to support risk-ranking beliefs; that is a subject for another study.

Another powerful use of frameworks was as a communications tool. Bridging the gap between IT thinking and business thinking has always been a cybersecurity challenge; many of the interviewed firms talk about using their framework as a communications tool to make the risks more concrete. As one CISO put it, the framework allowed senior non-technical business leaders to understand the approach and the needs; the framework allowed him to get funding, and to report progress in meeting expectations. Frameworks are valuable to another CISO because it is "fairly easy to discuss and to convey to different layers of leadership". Another CISO talked about how the framework makes it clear to senior management what their current risk rating is, and how much needs to be invested to bring risk down to a

particular level.

Framework development As mentioned above many firms have developed their own frameworks. At a high level all frameworks, whether standard (e.g. NIST) or custom, incorporate elements of business assets, processes, vulnerabilities, and probabilities. The differences between the frameworks presented in the interviews lies along a few dimensions:

- Their specific environment
- Costs of remediation
- Other internal or external knowledge (e.g., threat information)

Here we hope to shed a little insight into how a few firms went about developing frameworks.

The first case to discuss is a financial firm. The director of information security for this firm takes a broad, systemic view of cyber risk management, thinking about where does security begin and end, and what does security mean for their organization.

His initial approach to developing a framework started by identifying 3–4 dozen domains that map back to FFIEC handbook domains and to ISO 27001 primary and secondary domains. He then evaluated the entire entity based on asset class and determined their strengths and weaknesses with respect to control abilities. More recently the entity has adopted the NIST framework, using several domains to help them assess the confidentiality, integrity and availability of data as well as the governance and strategy. The director says that these have many associated technology risk functions and they've spent effort to address the associated change management and strategy. The results of efforts become elements of a COBIT-style risk framework they use.

This framework is used to assess assets, controls and compliance across the entire enterprise. The results inform the work of cybersecurity-specific committees, compliance committees, operational risk committees and enterprise-wide risk committees. As a result, enterprise-wide policies and standards are developed, and the entire enterprise must adhere to these minimum baseline standards.

The director of information security says the frameworks helped senior-level business leaders understand the systemic approach; this understanding enabled him to get funding for his projects. The framework has also prompted a discussion around the real cyber risks in the enterprise as a whole, how they manifest themselves, and how to respond and recover once bad actors have penetrated their systems. To enable this, he spent an enormous amount of time translating frameworks into language that business leaders and managers could understand.

Another example comes from the health care sector. This started out as an extensive security audit by a third-party, which resulted in a comprehensive report that broke down the firm's risk areas into categories and offered recommendations for each area. The CISO had additional consultants come in to validate the statements in the report. From this the CISO developed a risk register of the risks the report identified as 'high' or 'medium'; the definition of risk used was the likelihood of that event happening over the next 18 months, and the potential impact. High risks would have a substantial impact on the ability of the firm to meet its objectives; medium risks would have a moderate impact.

Using this risk register he identified the top 20 risks and then looked at the firm's risk appetite and willingness to spend to put together a project roadmap to address these risks. He also used COBIT's Maturity Model to build a security maturity framework for the firm, and developed an assessment of where they were now and where they wanted to be in three years. He used these frameworks to justify projects; the CISO said that these frameworks created a lot of discussion at the leadership level.

Further examples of how CISOs create customized frameworks can be found in Section 8.

Security frameworks: the new checkbox? A few years ago a major driver of information security investment were lists of controls that were needed, and investments were made to 'check the box': e.g., 'we have antivirus!'. One of the shortcomings of the checkbox approach was that it did not lend itself to thinking critically about the cyber risks faced by the organization. The checkbox approach achieved compliance, but did not ensure risks were being properly managed. The security frameworks commonly used today invites executives to think rigorously about their organization from a risk perspective, and their widespread use indicates a general maturation of cyber risk management.

That said, there remains a concern that although CISOs are using a more mature tool, they may not be using it to gain a more critical understanding of the cyber risk stance of their organization. In effect, they might be using it as a more advanced 'checkbox'. We did hear examples of this during the interviews, where at least one CISO talked about their primary goal being to keep compliance with the framework as high as possible and to keep findings during audits low. Other CISOs directly applied standard frameworks across the enterprise, without first taking the time to understand the realities of the business units with which they lacked familiarity.

In this sense, the firms that are developing their own cyber-risk frameworks likely do have a better understanding of their cyber risk than the average framework user. Most of the firms that develop their own frameworks do so to better organize different views of risk, from different sources. These firms go beyond using a framework; they develop a custom

framework and go through the work needed to ask and answer the "where does security begin and end?" and "What does security mean?" questions.

5 How CISOs Deal with Asymmetric Information

One of the key barriers to cybersecurity identified by researchers has been the presence of asymmetric information. For example, if a firm cannot accurately assess the security level of products, then it could refuse to pay a premium for security. When this happens, the market can suffer a paucity of high-security products (as the vendors will not be paid their true value) and be flooded with low-security products[3]. Another way in which information asymmetries present themselves is by a firm's misunderstanding of the severity of threats. If a firm does not know how it is being attacked, it is very hard to correctly allocate budget to effective countermeasures.

We asked CISOs whether they felt they had adequate information to prioritize threats effectively and to select the best security controls. On both counts most respondents felt that while the information was far from perfect or complete, they have enough information to make the right decisions. Consequently, in the eyes of the CISOs we interviewed, asymmetric information does not present a significant barrier to achieving their goals.

5.1 Do organizations feel they have adequate information to manage risk and prioritize threats?

When asked directly whether they felt they had enough information to manage risk and prioritize threats, only 45% of CISOs responded with an unqualified "yes". However, on digging a bit deeper, those who answered "no" typically responded along the lines of 'I can manage the threats I know about, but I still worry about blindspots'. More than one invoked the Rumsfeldian concern over the threat of "unknown unknowns". This attitude reflects an acceptance that security can never be perfect, and while they express great confidence in the steps taken, they also know that some risks must be accepted rather than mitigated.

Why do firms have such confidence in their assessment of the threats facing their organizations? Much of this can be attributed to efforts to increase visibility to security threats. Many CISOs mentioned the use of third-party threat intelligence data feeds. Most operate a SIEM. Slightly fewer rely on data-loss prevention (DLP) technology, but for those that do not, the main explanation given was that they did not feel they had the capacity to take

[3]For more information, see R. Anderson, "Why information security is hard – an economic perspective", in *Annual Computer Security Applications Conference (ACSAC)*, pp. 358–365, 2001.

actions based upon the information a DLP product would return. So while an information asymmetry clearly may remain in this case, the decision was made explicitly to avoid taking on more information than can be acted upon.

Finally, several firms (notably in finance and energy sectors) reported that they are regularly briefed by colleagues in the federal government on security threats. Some CISOs even maintain security clearances directly for this purpose, or employ staff who have security clearances.

5.2 Do organizations feel they have adequate information to select the best security controls?

A related question is whether or not CISOs feel they can make informed decisions on selecting the right security control when choosing among competing offerings. 85% of CISOs said that they had as much information as they needed when selecting a security control. Where do they get this information from?

They don't get the information they need based on cold calls from sales teams. One CISO warned against the "fog of more". He is contacted by a vendor 10 times a day ("I'm not exaggerating"), each claiming that they have a tool to solve all their problems. He ignores these solicitations, treating them as noise. Instead, he starts with a defined problem, usually a gap identified by a framework, then explores the landscape to find candidate solutions to this problem, and then carry out a more thorough comparison among tools.

While CISOs might be able to resist the sirens' song from vendors touting the latest and greatest technology, senior management is not always so disciplined. Invariably, senior leaders come across news articles or conversations with others that suggest a particular technology may be promising, and they sometimes ask the CISO to evaluate the tool. In the words of one CISO, "what I always want to say, but don't, is if we have to change a strategy because of an article you read in the Wall Street Journal, you should probably fire me" because changing course would demonstrate a lack of strategy and vision in terms of cybersecurity investment.

What we found is that the reason most CISOs are confident that they can select the right security controls is that they have a process that they follow and have confidence to select the right tool. The frameworks identify what controls are needed where, and then the solicitation and evaluation helps identify the right product for them.

A range of strategies are used. For many large companies, the starting point is outside research from a third party such as Gartner or Forrester. 82% of CISOs reported using the Gartner reports, notably the Magic Quadrant, to identify a list of candidates and assess

strengths and weaknesses in terms of features and performance. 25% of CISOs reported using Forrester. Nearly all CISOs using these products were quite aware of their limitations, stating that these help pare down the field rather than make a final selection. It should also be noted that some CISOs at smaller organizations deliberately look for companies and products not covered by this outside research. The explanations why typically centered around the perceived higher cost of large vendors and the lesser requirements that these smaller organizations may have.

Many larger firms run a "bake-off" among finalists, where systems are deployed on a trial basis within the organization. This testing yields not only insight into the relative performance among the candidates, but also can identify how well the prospective components fit in with the existing infrastructure. Furthermore, the bake-off gives the security team a chance to test out which systems they are most comfortable working with.

Getting such buy-in from the security staff is essential. As one financial CISO puts it: "it doesn't matter how good the tool is if the program is in the drawer and not on the floor". This CISO takes it even farther, believing that most security technologies would be good enough so long as the right people and processes are behind it. With that in mind, his strategy is to issue an RFP but let the technical people within the organization help decide the finalists. This includes not only security staff, but also the rest of IT operations. Getting staff buy-in helps ensure that the product would be used to its full potential.

When asked for the most valuable type of information when choosing among security controls, the most common refrain was peer feedback.

5.3 Value of information sharing groups in mitigating information asymmetries

Nearly all US-based CISOs reported that they participated in geographic or sectoral-based peer groups with fellow CISOs. Many reported that their participation has been highly valuable, not only for high-level sharing of threat intelligence but especially for gauging others' experience with security products and services under consideration by their own firm. Peer feedback on products has been reported to be valuable in both winnowing down the field of contenders and for helping to select among finalists.

We noted that these groups were seen as less valuable outside the U.S., at least in their current state. International information-sharing organizations tended to be driven more by governments as top-down initiatives than bottom-up ones as often observed in the U.S. For example, a CISO for a British financial firm reported that he recently joined a government-led information sharing initiative, but that it was "early days" and too soon to

judge whether the collaboration would prove valuable. By contrast, every US-based financial firm we interviewed mentioned that the FS-ISAC was highly valuable in sharing high-level threat information.

6 Sector-level Differences and Similarities

One question we examined was whether there are significant differences in approaches to cybersecurity among the four sectors that were the focus of this study (Financial, Health Care, Retail, and Government). Do the different sectors focus on different threats, or use different methodologies for assessing and prioritizing risk? We used a few dimensions to guide our analysis: the reporting structure, change in budget, identified threats, prioritization approaches, management support, level of external interactions, and how far into their business they reach to understand enterprise risks.

With a few exceptions there is more commonality than distinction among the focus sectors. The exceptions are the Government entities interviewed, where the prioritization tended to focus less on risk and more on compliance, and the changes in cybersecurity budget did not track with the budgets in the other focus sectors (see section 7.1).

6.1 Reporting structures

One of the interesting themes that came out of our discussions was the organizational reporting structure. Whereas a few years ago the CISO would always report to either the CIO or CTO, today there's a range of reporting structures. There is a growing realization that the CISO role as currently construed might fit the risk silo better than the technology silo.

Role reporting to:	Finance	Healthcare	Retail	Government
CRO	1	1		
CFO	2			
CIO		2	6	4
CTO	1		1	
COO	1	1		
Board of Managers			1	

Table 1: Reporting structure by sector. The left column indicates the role that the CISO reports to.

Table 1 tallies the findings for the subjects we interviewed.[4] In both the retail and

[4]Note that the number of data points here and in Table 2 is less than 40 because not all interviews elicited responses to this question.

especially government sectors the available data shows a traditional CISO - CIO reporting structure. Greater variation is seen in both the health and financial sectors.

An emphasis on risk over technology particularly evident in the financial sector, where CISOs report to anybody but a CIO. Respondents reported to CROs, CFOs, CTOs and COOs, but none reported to a CIO.

One CISO says the only reason cybersecurity exists is to manage risk, and being bundled under the IT silo is the wrong place. Another finance CISO states that in order to be effective a CISO needs to be able to quantify information risk in terms of dollars; he reports directly to the COO. A third finance firm talks about the three lines of defense paradigm used in the insurance and financial sectors and noted that the CIO is primarily a 1st line role, while the CISO is primarily a 2nd line role and thus the CISO should be in a different silo than the CIO. This is semi-formally codified in England where the British Financial Conduct Authority (FCA) recommends the separation of information security from IT. Other sectors express additional reasons, such as increased visibility of cyber risk in the organization. A healthcare CISO noted that the likelihood and consequences of a data breach from a cost and damage to reputation standpoint demand a higher level of visibility in the organization, and that the CISO role needs to be more visible as well. Other CISOs have explicitly managed to increase the visibility of cyber risk by creating risk management committees whose members include C-level leaders.

Some CISOs nonetheless prefer to report to the CIO. One states that he would like to stay in the CIO silo due to the effectiveness of the CIO within the organization – he believed cyber risk would have the most visibility with that reporting structure. Another contrasted the limitation in executing technologies that implement policies when CISOs report to the legal counsel, as opposed to the CIO. "What I've seen in that space [when CISOs report to CLOs] is there's a lot of power to create policies, but accountability for the technical implementation and enforcement of that policy is difficult to do. And the level of visibility into what's happening at a technical level can sometimes get obscured because there's a natural fear of sharing ugliness outside the family, if you will." The CISO continues, "one of the things that is important about having the security function align with the IT organization is that I control enterprise security policy, I control the systems that implement and enforce that policy, I control the people and processes that respond to issues and threats to the environment, and I control direction of the team that performs the recovery activity in the event that something goes wrong. So by being able to touch all of those and have direct accountability for them, I feel like I have better continuity in being able to implement a program that isn't just a policy, it's a policy that's backed up by real technology implementation."

6.2 Budget changes by sector

Change in Cybersecurity Budget as a Function of Business Sector				
Change in budget	Finance	Healthcare	Retail	Government
Increase	III	III	III	
Same			FF	III
Decrease				

Table 2: Change in cybersecurity budget over the past two years by business sector. These data represent the responses given by the interviewees; e.g. an interviewee saying 'it hasn't really changed' would be counted in the 'Same' row. The right column indicates the role that the CISO reports to. An 'I' indicates an individual firm, an 'F' indicates a firm based outside the U.S.

Table 2 reports whether or not respondents have experienced a change in budget over the past two years, broken down by sector. We can see that regardless of sector, private-level firms reported an increase in budget. Most firms indicated that cybersecurity was becoming a major focus, either as a result of their own data breach experience or those of other firms such as Anthem or Premera. Those and other events have clearly changed thinking in most firm's senior management about cyber risk management.

Government was an exception, where those interviewed reported no change in budget levels. This reflects overall trends in the government budgeting process. For more, information, see Section 7.1. Interestingly, two foreign retailers also said that their cybersecurity budget had not changed.

6.3 Foreign cyber risk management is all over the map

We have interviewed CISOs from several countries as part of this study. Compared to their non-U.S. colleagues the U.S. CISO interviews were quite similar: they were aware of the same issues, had the same drivers, and largely shared the same experiences in terms of identifying, prioritizing, and getting cyber risk efforts funded. The non-U.S. CISO interviews exhibited a vast range of approaches. One CISO's approach would be best characterized as 'post-cyber-security' in the sense that the CISO had surmounted the cyber aspects of information security and was concerned with broader, pan-information security. Two interviews from another country brought to mind interviews in the U.S. from 10 years ago: cybersecurity was not a big deal; we will spend more time worrying about it when a cyber event happens to someone we know.

This range of attitudes is quite intriguing; we are very interested in understanding the underlying cause and how to promote individuals to take a rational approach to cybersecurity

(assuming they are not already doing so).

7 Special Challenges for Government CISOs

We interviewed one local (a very large county), two state-level, and three federal executives. From these conversations it became clear that the CISO role in government presents unique challenges and responsibilities not seen in the private sector. Whereas in industry, management support for cybersecurity has translated to access to budget, this is often not the case in government. Senior leaders in government recognize the importance of cybersecurity, but structural issues within the bureaucracy often inhibit adequate and timely prioritization. We focus our discussion on challenges facing U.S. federal CISOs, though the challenges did come up in other interviews with government officials, but in contexts specific to their jurisdiction. We have left many of those details out in order to preserve the anonymity of the subjects.

Note that because the number of government CISOs we interviewed is small, relative to the overall sample size, we caution against extrapolating generalized conclusions from the findings presented. Our goal here is to relay the experiences of the subjects we interviewed in hopes of shedding light on the challenges they face.

7.1 Challenges to the budgeting process

Money is always tight in government contexts, and cyber is no exception. Cyber budgets are part of a bigger budget, and adding funding for cyber almost always means defunding something else that could be providing a service rather than protecting infrastructure.

In addition, the extended government procurement cycle (typically 3 years long) means little flexibility to divert resources to protect against emerging threats. One could say that budgets and investments are based on last year's threats, at best. As one federal CISO said, it "was difficult to move from actionable intelligence (when I knew the bad guy was there) to legitimize procurement in something sooner than a three-year cycle. ...If I saw something in 2014 I'd have to put it in my 2017 procurement plan". This CISO contrasted this experience with his time in private industry, where his threat intelligence is weaker than in government but he can act more quickly when the need arises.

Another federal CISO bluntly stated that "the appropriations process is killing us." Why is that? The CISO lists several reasons. First, moving budget is harder than it used to be. Any budget shift over $500K requires Congressional approval. Prior to this requirement, the CISO could easily repurpose unused budget from say, unfilled FTEs to the purchase of technology or services. Second, full acquisition approval cycles are required for any purchase

over $3,000. Planning these expenses out far in advance is onerous at best, and impossible when new threats emerge. Third, uncertainty over budgets can lead to less effective spending. Single-point solutions can be very expensive, and the CISO reports that he is often required to "peel these back" because he can't fund the ongoing maintenance. This CISO now tries to get multi-function tools that are cheaper and better, but before he can get rid of the old, expensive and less-functional tools and bring on the new ones, he must fully depreciate the old ones or develop a retirement plan and get that approved. But if a tool is retired, there is no guarantee that he will get the money from that to purchase the next tool. So the choice often comes down to carrying on with an expensive, less effective tool or taking the chance in hopes of getting a cheaper, more effective one.

Due to these and other issues, he estimated that his agency is at least two years behind the curve on cybersecurity. He therefore concludes that "the process is painfully broken."

A related budgetary challenge that exists arises from the relationship between agency and department-level CISOs.

7.2 Tensions between agency and department-level CISOs/CIOs

In the US federal government, CISOs and CIOs are appointed for departments and well as their constituent agencies. For example, there is a CISO and CIO for the Department of Transportation, as well as for the Federal Aviation Administration, Federal Highway Administration, and the other 11 agencies under the DoT. In principle, departmental-level CISOs and CIOs have authority over the agency-level officers. However, in practice, departmental-level officers have limited budgetary control, and so they cannot implement strategic investments across the department. Consequently, most security efforts are led by agency-level CISOs, and there is often a lack of coordination between the department and agency level.

One federal CISO sums up the dilemma facing departmental-level CISOs as follows: "They don't have money, they don't have people, and they all report to CIOs. So security is subject to the imperative of keep the system up, keep the mission running, and oh yeah security if there's time and interest."

Even at state level there can be disconnect between authority and budget. One state-level executive reported that while his office has responsibility for ensuring the security of IT systems, counties choose what IT systems to install because they control their own budgets. The officer is then left with the challenge of securing many different systems, without budget or central oversight.

7.3 Tension between compliance and security in oversight process

Oversight comes in the form of an audit for compliance to a set of standards and this year's operational plan; completing the audit requires a very significant portion of the time available over the year.

The FISMA process centers on carrying out periodic Security Certification and Accreditation (C&As). In the words of one federal CISO, "The whole FISMA and C&A process was horrendously outdated". CISOs pointed out two key problems: the slowness of completing the process rendered the results immediately outdated, and the time and budget required to comply distracts from the mission to improve security.

For example, one CISO explained that he managed several hundred systems subject to FISMA C&A. The inspector general (IG) would begin the review process in January, run through their sampling of tests, control selections and processes. They would define their testing categories, and by June or July, the IG would come back with initial reports, in hopes of finishing up by August or September. The IG would deliver the report to the CISO in November, who would have to come up with action plans (POAMS), get those signed off on by the secretary and into their system for tracking, which leaves just enough time off for the Christmas holiday. By late January, the IG would start asking about how they were doing with all those weaknesses they found in last year's report.

Fortunately, leaders within the government are exploring new ways to improve security. According to one CISO, leaders recognize the need to "get away from creating books that say we are safe, which is in fact taking resources away from actually making sure the government is try to protect its networks." One such effort is the Continuous Diagnostics and Mitigation Program, led by the Department of Homeland Security. Multiple CISOs pointed to this process with optimism, hoping that the measurements enabled here might even eventually displace the traditional FISMA approach with more timely feedback.

7.4 Government CISOs always report to CIOs

These CIOs are both political appointees and career staff. In either case they are more focused on operations than they are on cyber risk. This is the same dynamic as was outlined above.

7.5 Effective government CISOs get creative

Despite the challenges outlined above, we also found in our discussions that effective security officers get creative in order to get their jobs done. For example, one CISO recounted how he

has repurposed existing equipment to deploy security controls running open-source software. Doing so enables him to sidestep the appropriations process and deploy a needed control quickly. Another CISO explained that in order to win budget for critical investments outside the three-year cycle, he would find vulnerabilities in agency systems and demonstrate the problem in presentations to senior management. By making the threat "real" to decision makers, the CISO could effectively make the case that he needed support now.

8 CISO Mavericks

Over the dozens of interviews conducted, a few subjects stand out as exceptional in their approach to cyber risk management. In the past we've always found that these 'mavericks' provide great clarity and insight into the practice and possibilities of cybersecurity; these are the conversations that are most likely to impact our assumptions and thinking. We've chosen to share a few of these.

Maverick #1 The first is the CISO of a firm that thinks in terms of the 'three lines of defense' paradigm as mentioned on page 19, and the CISO is very clear about the distinction: he carries the responsibility for operational security, the threats, but not risk. Although many firms have the CISO role responsible for managing cyber risk he firmly thinks that cyber risk should be handled by a 'Chief Information Risk Officer' — CIRO. This CIRO role would define risks in terms of annual expected loss. He thinks this is the best way to quantify risk (as it is a metric that everybody can understand).

Presently the head of IT risk in the organization creates policies from a risk perspective; these are broad statements such as "there must always be authentication", but does not get into the 'how' part. The CISO deals with the 'how': "Authentication means...". At this level he can best translate the stated policies into practical implementations, what really happens in the systems taking into account system limitations. He thinks of this in terms of 'principle-based' and 'effectual' policies, where 'principle-based' policies look more at a strategic level (e.g., reducing firm risk resulting in reduced capital requirements), and 'effectual' policies focus on implementation.

This focus on implementation is based on a firm view of the threats. This leads him to push back on requests from within the organization to implement a particular control; he will work to understand the underlying threat, and then work to understand if that is the best place to invest money from the firm-level perspective. He used biometrics as an example. Managers in the firm were asking to have it put in place, saying 'everyone else is doing it, why don't we?'. He thought that it was not a wise investment, as biometrics wouldn't do

anything against an attack, it would not increase the security posture and would raise the help desk costs. He thought the money that would be used for biometrics would be better spent against other threats.

He employs an "ethical hacking team" that conducts internal and external penetration testing. The primary motivation for the team is to build trust in the company by verifying the implementation of his security controls. He says if he can't put a purely informational website online which is secure, how could he expect a customer to trust them in other business contexts. He believes that this team has made the biggest positive impact on improving security in the company. Their findings raise awareness throughout the organization, and help drive security priorities by offering a visual representation of a business case that is "easier to digest than a spreadsheet".

He is also averse to large changes across the firm, such as installing new firewalls. From experience he knows that it would take the better part of a year for the entire firm to adopt and adjust to the new technologies; during the transition they will be more at risk. As a result he likes to space out the three-year lifecycle of technologies such that only 1/3 of the firm is involved in a disruptive upgrade at a time.

For him, threat prioritization is based on the expectation of external customers, not internal colleagues. When spending against those threats, he is only concerned with the effectiveness of the results (i.e. reducing risk) than with the efficiency.

Maverick #2 The second CISO maverick is also from the financial industry. A couple of years ago, the firm's CISO evaluated the changing cybersecurity threat landscape. He concluded, with external consulting assistance, that the firm needed to re-think their approach to cybersecurity. As the CISO puts it, "[It] seems like we've all been engaged into a cyber arms race for which we have no option to opt out or seek treaty. There's no other choice but to respond to that threat."

To respond to this challenge, he developed a framework for the firm. While the framework is a combination of NIST, ISO, SANS and COBIT, the framework was really established by the attack vectors the firm and industry were seeing. The CISO explicitly wanted to shift the risk organization culture from a compliance and governance-centric focus to much greater primary focus on deep defensive tooling and skills with deployment consulting.

This resulted in a Framework that identified their four central risks:

- Loss of confidential data
- Financial account compromise
- Business continuity

- Regulatory non-compliance

The framework also identifies a few primary threat agents, including:

- Hacktivists
- Organized crime
- Nation–State
- Insiders

For each of these threat agents, their attack vectors and attack phases he and his team mapped the cyber defensive tooling needed to detect or prevent at each attack stage. They prioritized capabilities based on the breath of coverage across vectors and attack stages.

They broke down the threat vectors into distinct attack phases: recon, weaponize, deliver, exploit, command and control, and exfiltrate. Again, they worked to define the set of ways that each of these attack phases might happen, and with that knowledge what approaches could be used to disrupt these phases. After completing this analysis, he says that there are an almost infinite set of ways an attacker can get a foothold, but the later stages of the attack are the same across attack vectors, and that's what he tried to disrupt first. For example, the bad actors all need to exfiltrate the data.

To execute this strategy, he established the role of defensive coordinator; they are breaking down these attack phases and identifying a concert of tools that are orchestrated to stop these phases even in the case of the failure of a single tool. He thinks in terms of a layered, full-lifecycle defense; he talks about a 'fabric' of cyber defense.

He talked about taking a 'start-up' attitude with this challenge; he very much did not want to understand his problem through the eyes of others but rather to develop an understanding from the perspective of the treat agents. For example, he purposefully avoids CISO forums because he didn't want to be initially bound by the thinking of other CISOs. When selecting which tools to invest in, he not only uses Gartner or Forrester, but goes to Silicon Valley to talk to VCs about the technologies they're thinking about, and where they are investing.

Maverick #3 We started off this section with a CISO who made clear he did no risk-based policy development, only implementation. Our second 'maverick' implemented a framework for disrupting attacks driven from the attackers view. For our final 'maverick' we present the flip side: someone who does no implementation, but does risk-based policy development. This individual is the VP of security compliance and audit at a firm that manages sensitive

data. He and his team defines policy for the firm's data and applications, the firm's VP of security will then implement these policies. The VP of security compliance and audit also defines controls, group and network policies.

Each new project at the firm has an associated 'workbook'; this workbook defines the system to be built and lays out what data it will contain, where it's going to sit in the suite of applications, who will have access, and other defining characteristics. Based on this information he and his team decide where the application should sit in the IT environment. When they consider the placement they think about it from a breach perspective – they assume that the application will be breached and consider the consequences. They develop all the access controls, including for any shared data or database access.

He has a deep background in penetration testing – an activity he still practices directly. This background informs his world view of cybersecurity; he says, "I don't believe that email, the internet, anything is secure, period". As a result, he says he trusts nothing: in addition to specifying the policies, he continually tests to see if these policies are in place by pen testing all the firm's outward-facing applications from an external location. He does research and analysis on zero day attacks and thinks about and implements controls to manage various zero-day scenarios. He says he's broken enough systems to know it doesn't take a tremendous amount of effort to get through the perimeter of a company, and therefore does not spend a lot of time thinking about firewalls and perimeter controls. He knows perimeters and defenses are being broken every day, and instead wants to be nimble enough to protect their environment and data once the perimeter is breached: "if our controls are what we have open at the firewall and that's how we protect things, we will never survive because a breach we can't control". He wants to be better, smarter, and faster.

Budgeting – not mavericks but still exceptional. It would be unfair to characterize the budgeting process by these individuals as wildly independent, but their budgeting process is instructive. The CISO in the first case could not recall or even estimate the cybersecurity budget, as it is not a separate item, but is what he calls an 'attribute' of business — part and parcel of doing business. It might meet the 'baked-in' security definition. The second CISO did get a more traditional budget. After defining the cybersecurity projects based on the framework he developed, he and the CIO walked into the CEO's office, explained what they had done, and walked out with 3 year's funding for their cybersecurity projects. Finally, the VP of security compliance and audit has no budget. In his current situation he's funded through overhead, and can fund projects up to $1 million without asking for budget.

The New Traditionalists. Having pointed out what came across as outliers, what does an "in-lier" look like? While we want to be clear a wide range of approaches are used by the interviewed CISOs, there are some common patterns that we will make use of to define the in-lier. The CISO of an in-lier would probably not report to the CIO (but to whom they would report is variable). They would use a combination of frameworks to understand the risks of the enterprise, prioritize cybersecurity efforts, and to communicate this to senior leadership. This combination of frameworks would utilize the NIST framework to understand the risks more abstractly, and the ISO framework at a more concrete level. These frameworks would be applied mainly at the enterprise level, with not much interaction with BUs. The results and planned cybersecurity projects would be presented to a cybersecurity oversight board that would include the CEO, CFO, CIO, CISO, and other senior leadership. The CISO would have asked for this oversight board to be created, as it would give him direct access to the most senior leadership. This leadership would be supportive of the creation of this oversight board and the CISO's efforts, as they have been sensitized to what can happen to firms that have breaches, and do not want to be that firm.

9 Conclusion

We explored how firms identify, prioritize, and invest to manage cybersecurity risks with 40 executives using a semi-structured interview format. Above we have reported in detail on interviewee responses to our questions; here we conclude by presenting key take-aways.

Support of senior management is quite high in private sector. With very few exceptions, senior management understood the importance of cybersecurity efforts. This led to support not only at the senior management level, but in many cases at the board level as well. When asked what has made senior management so supportive the most common reason given was recent widely–publicized breaches such as the Anthem breach. These events seem to have greatly raised the awareness of what impact a lack of cybersecurity can have.

Getting budget for cybersecurity efforts is not as much a challenge as is resourcing cybersecurity projects. As a result of senior management support budget is generally not a limitation for non-governmental entities; some interviewees would say that their senior management wanted to move faster than the CISO thought was advisable. In some cases senior management would not allocate the full requested budget due to concerns that the CISO's organization could not execute the number of proposed projects; they weren't concerned about the budget but about the size of the effort being more than the

available resources could reasonably complete.

Finding qualified personnel is a key challenge. Many interviewed CISOs talked about increasing the size of their teams significantly – one CISO talked about increasing headcount by 20 – and the challenges with finding qualified personnel to do so. Interviewees spoke of open positions, and of deciding they will not be able to hire experienced cybersecurity professionals and instead hiring recent college grads that will be trained internally. This lack of talent impacts the utility of cybersecurity applications: one CISO stated that he believed he was not making full use of his cybersecurity applications because his staff was not able to make use of all the features those applications — this is a skills and usability issue.

Frameworks are at the center of defining risk perception and investment. Most every cybersecurity director we spoke to uses a framework to define their firm's cybersecurity status and to prioritize investments. These frameworks ranged from well-known frameworks such as ISO and NIST to homegrown frameworks that might be some combination of existing frameworks or completely custom. Some CISOs also value frameworks as a powerful way to make clear to senior decision makers the business risk they face due to cyber events; this understanding of the potential business impacts enabled the CISOs to effectively present the case for projects, and allowed them to report progress.

There is much more focus on process than outcomes. A focus of this research was to see if outcome measures were used in budgeting decisions (e.g. ROI). The interviews themselves made clear that there was much more focus on process measures than outcome measures. A focus on controls – finding and fixing gaps between current and desired cybersecurity posture – dominates. There is much less focus on the actual results of cybersecurity efforts, such as examining costs and the effectiveness of controls. This may be due to the widespread use of frameworks which promotes the use of process measures.

There are very few notable differences between the sectors studied. This study focused on the financial, health care, retail and government sectors. While they have much in common in how they approached the cybersecurity challenge, there are a couple of notable differences. First, the three-year budget cycle in the U.S. government sector as well as the current auditing requirements are a challenge for government CISOs that their private-sector colleagues don't have. Second, the financial sector has made the distinction between operations and risk management in a much more concrete manner than the other sectors studied. In the financial CISO reporting chains we encountered, the CISO never reported to

the CIO, which is not the case in the other sectors.

The use of intelligence (third-party or other) is widespread. One of the more promising findings is that there is good deal of information sharing regarding cybersecurity. This ranges from informal venues such as CISO talking shops to more formal structures such as ISACs. Topics discussed included threats, as well as opinions of cybersecurity applications/devices. Many interviewed firms were getting threat intelligence both internally from their SIEMs and externally from third-party threat intelligence providers. We heard of multiple individuals having security clearances and of having access to classified threat intelligence. This sharing of intelligence might be most robust in the U.S.; one foreign CISO talked about it being 'early-days' for his country's ISAC-equivalents. Another foreign CISO expressed some frustration with threat-sharing and incident assistance by his country's intelligence and law services; he said the U.S. FBI was 'only a phone call away'.

Overall we think that CISOs have robust resources and processes to manage cybersecurity; unfortunately bad actors also have robust resources. We believe that this is a period when many firms will elevate cyber to being a first-class risk which will lead to a significant adjustment to the role of the CISO.

We conclude by noting an unresolved disconnect. On the one hand, CISOs express high confidence in frameworks and their ability to identify and deploy the best controls to improve cybersecurity for their organization. On the other hand, the steady drumbeat of high-profile breaches shows no sign of abating. We speculate that this contradiction may result from an overconfidence in the process-based measures and a corresponding lack of emphasis on measuring secure outcomes. Explanations for why we observe this phenomenon are likely behavioral, and understanding why is surely to be an exciting opportunity for future research.

Acknowledgments

The authors gratefully acknowledge support from IBM, who sponsored this research project. This paper represents the position of the authors and not that of IBM.

A Interview Questions

A.1 Grounding Questions

- Please briefly describe your background.

- Please briefly describe the reporting chain in your organization. Where does risk roll up?

A.2 Macro-level Questions

- How has your infosec budget been changing over the past couple of years?
- What are your primary concerns from a cybersecurity standpoint?
- What do you see as the biggest threats for your company?
- How do you identify which threats are most important and prioritize accordingly?
- What factor is most important in driving cybersecurity investment: cost reduction, compliance obligations, perceived risk reduction, general process improvement, or something else? Please elaborate.
- When thinking about infosec spending decisions, are any evidence or metrics used in making cyber investment decisions?
- Do you use ROI? If so, how do you find it useful? If not, why?
- Do you feel that upper-level management adequately supports cybersecurity investment needs? Why or why not?
- Has the degree of support changed over the past few years?
- If you get push-back, how does the conversation go?
- Do you feel like you have adequate information in managing overall cyber risk and prioritizing accordingly? Is there any way in which this could be improved?

A.3 Micro-level questions

- Can you talk about one or two of your most recent large cybersecurity projects?
  - Did you employ any of the metrics and measures just discussed?
  - What was helpful about them?
  - What was left wanting?
- When focusing on a solution to a particular problem (like the one covered in the recent project just mentioned), how do you choose between competing solutions. Is it based on:

  - price
  - superiority of technology (if so: how was this determined)
  - vendor leadership according to 3rd parties (Forrester wave or Gartner magic quadrant)? Which if either?

- Do you feel like you have adequate information available to make an informed choice between products? If not, what other information would be helpful?
- How do you evaluate security investments after they are made? Do you use evidence-based measures (reduced attacks, etc.), ROI, etc? How do you know it's working or not?
- Do you close the circle by tracking the change in the metrics used to justify the investment? (for these cases, what were your results relative to the metrics?)

At the end of the interview, participants were asked a final series of questions:

- Do you feel like your organization is spending too much, too little, or about the right amount on cybersecurity?
- Do you feel like your peers are spending too much, too little, or about the right amount on cybersecurity?

Participants were then given a "pop quiz" handout, which listed drivers of security investment and prioritization approaches. They were asked to rank (in order) their top three choices. Finally, they were given the opportunity to list an metrics that they use.