

In Practice



More is Not Always Better: A Value-Based Approach to Cyber-Risk Oversight

By Nate Fick, James Lam, and Shelley Leibowitz

In September 2017, consumer credit reporting agency Equifax admitted to a massive data breach, alleged to have occurred earlier in the year, which compromised the personal information of more than 145 million Americans. Over the next several weeks, the company announced the departures of its chief information officer, chief security officer, and—finally—its chief executive officer. Equifax’s market capitalization declined by approximately 25 percent, and it is the subject of a large and growing number of class action lawsuits.

Much attention has been paid to the claim that Equifax fell behind on patching known security vulnerabilities, but major breaches aren’t tied to a single factor. Security in large organizations is expensive and complex, and companies can devote significant resources to cybersecurity without mitigating the applicable risks. In short, more is not always better. How can companies not only protect themselves, but also enhance value through effective cybersecurity?

A new, value-based approach to managing cybersecurity using techniques commonly found in enterprise risk management (ERM) programs is presented here. First, we examine current cyber-risk management practices, which are focused on adding more defenses. We call this the “risk-aversion approach” and explain how and why it’s failing. Next, we lay out a “value-based approach” that is focused on quantifying cyber risk and integrating it into ERM. Finally, we discuss the board’s role in cybersecurity and offer five recommendations to improve a company’s overall cyber security posture.

Risk Aversion is Not Working

The Equifax data breach was not an isolated event: cybersecurity across most large enterprises today is in a state of failure. According to a study published by Duke University, more than 80 percent of companies have been successfully penetrated by attackers, and the average

“dwell time”—the time from when the attacker gets into a network to the time of detection—is greater than three months. Another study by Juniper Research states that the costs of cybercrime are expected to grow from \$500 billion today to \$2.1 trillion in 2019. At that projected level, cybercrime would rank among the top-10 countries in gross domestic product.

These failures generally are not due to a lack of focus or resources. Companies take cybersecurity seriously. They have appointed chief information security officers (CISOs), recruited cybersecurity experts for their boards, increased their risk budgets and insurance coverage, and deployed cutting-edge products. Despite these efforts, they are losing the battle.

There are four main reasons for the systemic failure of cybersecurity in large enterprises: the structural advantage that attackers have over defenders, the inertia of failing and fragmented approaches to information security, the growth of underlying

cyber risk, and ineffective oversight at both the management and board levels. Let's examine each of these four reasons.

A dollar of offense beats a dollar of defense. Attackers have an asymmetrical advantage over defenders. Defenders must be right always, while the attackers need to succeed only once; defenders must operate within the constraints of laws and regulations, while attackers do not. Moreover, the barriers to launching high-value, sophisticated cyberattacks continue to fall. Techniques and capabilities that were once available only to nation-states have proliferated across criminal groups, hackers, and others seeking to profit or cause mayhem in the digital domain.

The inertia of failing solutions. Most companies view security as largely a downside risk. Few businesses believe they will win in the market based on having better security, but they fear losing if they are shown to have worse security. This downside risk perception contributes to a highly conservative, "buy one of everything" approach that may satisfy compliance requirements, but doesn't necessarily result in better security. The rapid, parallel evolution of digital infrastructure and the threat environment has resulted in a highly fragmented vendor landscape where the average CISO of a large company has more than four dozen security vendor relationships.

Growing cyber risk. The problem is not getting better. The underlying cyber-risk profile for companies will continue to grow, driven by several factors. Companies will face greater *exposures* from device proliferation, including the internet of things (IoT), mobility, robotics and artificial intelligence, and infrastructure as a service (IaaS). According to research from Gartner, as many as 8.4 billion connected things were in use worldwide in 2017, an estimate that has increased by 31 percent from 2016, and that number is expected to

reach 20.4 billion by 2020. Companies also face higher *probabilities* from the proliferation of advanced hacking capabilities; more severe *consequences* from the rising value of intellectual and digital assets; and greater *financial and reputational risks* from higher customer, regulatory, and public expectations around privacy and data protection.

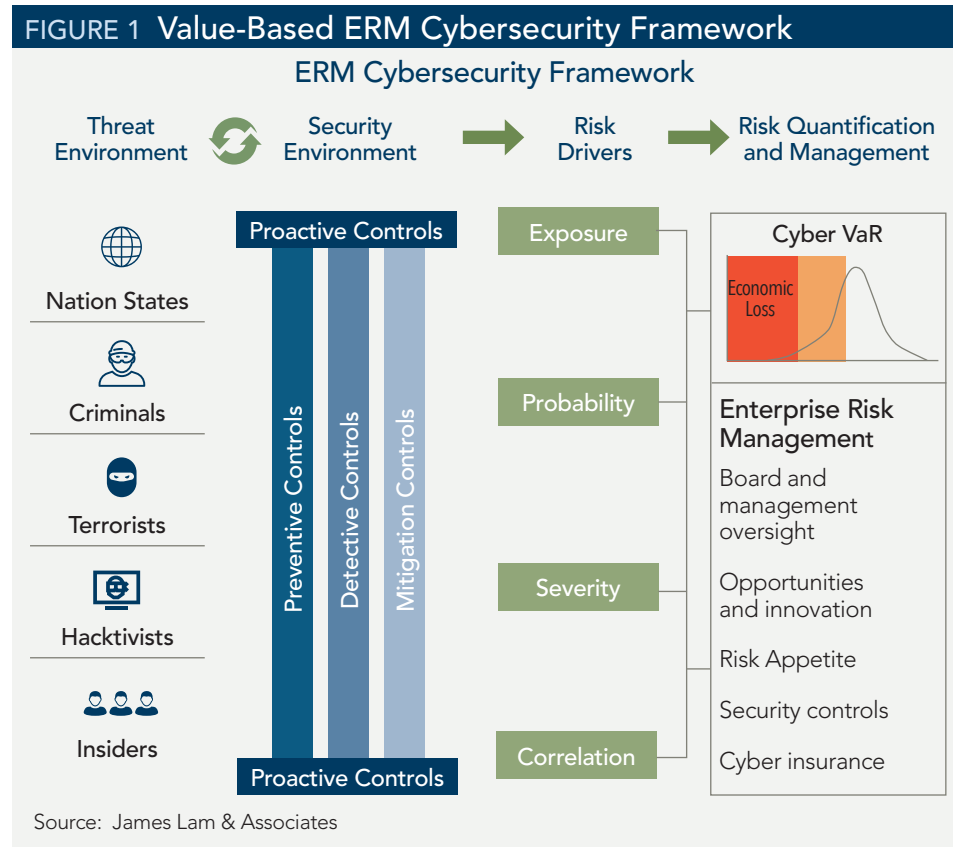
Ineffective governance and oversight. While cyber risk is a top concern for boards, most don't have the appropriate expertise to exercise effective risk governance and oversight. According to the 2017–2018 NACD *Public Company Governance Survey*, only 12 percent of boards believe that they have a high level of cybersecurity knowledge.

Current cybersecurity frameworks don't adequately serve the oversight roles of corporate boards. These frameworks are focused on CIO/CISO needs such as

maturity level, risk assessment, and security standards and processes, but they don't properly address board-level concerns such as overall program effectiveness, risk appetite and metrics, and capital management. Given that these frameworks and related gap analyses almost invariably dictate greater spending on cybersecurity, it becomes difficult for boards to provide guidance for effective allocation of resources across enterprise risks, and within cyber risk specifically. More spending doesn't equate to greater security or an optimal risk profile.

A New Approach: Quantify Cyber Risk and Embed it into ERM

Given the current state of cybersecurity, we advocate a fundamental shift in objective setting, risk analytics, and decision making across the enterprise. Figure 1 provides the



value-based ERM Cybersecurity Framework. The current “risk-aversion approach” implemented by many companies focuses solely on building up the security environment to protect against cyber threats (the left half of Figure 1). While protection is essential, it is also insufficient in the context of ERM and value creation.

From risk aversion to value creation. The objective of ERM should not be to minimize or eliminate risks. Rather, it should be to accept the appropriate risks that provide attractive returns. A “value-based approach” meets this broader objective by integrating the key risk drivers, ERM requirements, and the upside opportunities (the right half of Figure 1). The board and management can make more informed business and risk management decisions based on a better understanding of the impact of those decisions on the company’s risk profile. However, better decisions must be preceded by better risk quantification.

Cyber value-at-risk. “What gets measured gets managed” is a core principle long held in all aspects of business, including risk management. The ability to quantify risk forms the foundation of modern risk management, including value-at-risk (VaR) models. VaR is defined as the largest potential loss for a risk given a probability or confidence level. Risk managers use these models to quantify market risk, credit risk, and more recently, operational risk. In essence, VaR models provide a “common currency” for different risks by measuring potential loss with a consistent methodology.

Common risk drivers. Risk managers should implement cyber VaR models to improve risk quantification. While each risk has unique characteristics, there are four underlying risk drivers to support risk quantification: loss exposure, probability of occurrence, loss severity, and risk correlation.

- The *exposure* to cyber risk—the maximum economic damage, including financial and reputational losses—depends on the value of digital assets and how critical information security is to the company’s reputation.

- The *probability* of a cybersecurity event such as data breach depends on the sophistication of the attack relative to how effective *preventative* controls are. Companies can assess probability by penetration testing, red team/blue team vulnerability exercises, and independent cybersecurity ratings.

- The *severity* of a cyber risk event depends on how effective *detective* and *mitigation* controls are—the breadth and depth of the breach, dwell time before detection, and the response time to remediate the breach. The longer it takes to detect and fix the problem, the greater the severity.

- The *correlation* element in cyber risk reflects the relationships between internal and external risk drivers, such as human behavior, hardware configuration, network segmentation, and data storage. Any central points of failure make it more likely that a successful attack can bring down an entire system rather than individual components. Reliance on third parties raises the risk of indirect attacks and the combined failure of internal and vendor systems.

These four risk drivers support the quantification of any risk. Figure 2 shows the equivalency of risk drivers between market, credit, and cyber risks. By leveraging existing methodologies, a cyber VaR model can help quantify risk exposures and risk-return tradeoffs, and support capital allocation, risk mitigation, and risk transfer decisions.

Embed cyber risk into ERM. While cyber risk is complex in scope and scale, it is one of several enterprise risks along with strategic, financial, operational, and reputational risks. Boards and senior management can gain better control of cyber

FIGURE 2 Common Risk Drivers for Potential Loss

Risk Driver	Market Risk	Credit Risk	Cyber Risk
Exposure	Investment portfolio	Loan portfolio	Digital assets portfolio
Probability	Probability of loss or gain <ul style="list-style-type: none"> ■ Market price volatility 	Probability of default <ul style="list-style-type: none"> ■ Economic conditions ■ Credit ratings 	Probability of breach <ul style="list-style-type: none"> ■ Threat vectors ■ Preventative controls
Severity	Holding period <ul style="list-style-type: none"> ■ Market liquidity of investments 	Loss in the event of default <ul style="list-style-type: none"> ■ Collateral rights ■ Bankruptcy rights 	Loss in the event of breach <ul style="list-style-type: none"> ■ Breadth and depth of breach ■ Dwell time ■ Risk mitigation time
Correlation	Price correlations <ul style="list-style-type: none"> ■ Asset allocation ■ Position concentrations 	Default correlations <ul style="list-style-type: none"> ■ Loan concentrations ■ Country and industry diversification 	Threat and control correlations <ul style="list-style-type: none"> ■ Attack patterns ■ Data and network segmentation ■ Central points of failure: IT infrastructure, supply chain

Source: James Lam & Associates

risk by integrating it into an overall ERM framework.

Prior to the introduction of ERM in the 1990s, risks were managed in separate organizational silos. However, the siloed approach comes with many pitfalls, chief among them the inability to evaluate the relative importance and interdependencies across risks. Companies misallocated resources, spending too much on minimizing insignificant risks and not enough on more material risks. Over the past 20 years, companies across all industries have adopted ERM as a more effective approach to risk management. Unfortunately, as a newcomer, cybersecurity has grown in its own silo at many organizations.

An integrated, quantitative approach to cyber risk provides capabilities and efficiencies that are impossible to achieve if cybersecurity is managed as a siloed IT or security issue. These benefits include evaluating cyber risk comparatively to other enterprise risks; allocating risk budgets more effectively across risks and within cybersecurity; assessing key risk and control interdependencies; and determining whether the company should buy cyber insurance or self-insure.

The Board's Role in Cybersecurity

Cybersecurity in practice is management's job. The board's role is to provide effective risk governance and oversight, as well as credible challenge to management. As independent directors, we are concerned with addressing key questions such as:

- Is our cybersecurity program appropriate for the size and complexity of the organization?
- Does the cybersecurity program align with the overall business strategy?
- What is our overall cybersecurity risk policy, including risk appetite and tolerance?
- How do we know if the overall cyberse-

curity program is working effectively?

- Do we have a crisis management and communication plan in case of a breach?

Moreover, directors also must balance the downside risks with upside opportunities. New technologies are the lifeblood of business innovation. Being risk averse is not an option. According to research from the McKinsey Global Institute, "the most digitally advanced parts of the economy have increased their productivity and boosted profit margins by two to three times the average rate in other sectors over the past 20 years." Consider the speed of innovation: Amazon is reported to have a code release every 11 seconds, Facebook twice a day, and Google multiple times a week.

We offer our board colleagues five recommendations for consideration:

1. **Integrate cyber risk into the overall ERM program.** Cybersecurity should be an integral part of the governance structure, risk analytics, risk mitigation strategies, and monitoring processes in place to support ERM. We note that the very first key principle discussed in the *2017 NACD Cyber-Risk Oversight Handbook* is, "Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue."


2. **Focus on the basics.** The overwhelming majority of data breaches took advantage of known vulnerabilities. Directors should ensure that fundamental controls are in place for basic cyber hygiene, including patching programs, strong password policies, administrative privilege restriction, and end user training and behavior monitoring. People and culture should also be front and center of the program.

3. **Establish a cyber risk policy with clear risk appetite metrics.** An aspirational policy with general guidelines is insufficient to govern cyber risk. An effective policy must have clear definitions for cyber risk, key risk metrics, and risk tolerance levels. Expect

management to clearly define its cybersecurity strategy, plan, and policy, including quantitative definitions of risk appetite.

4. **Demand an effective board risk report.** A recent survey conducted by Nasdaq found that 91 percent of directors cannot interpret reports presented on cybersecurity. Qualitative risk assessments, heat maps, and maturity models are inadequate to support effective board oversight. A board-level cyber report should include commentary and metrics on the threat environment, risk exposures against risk tolerance levels, and effectiveness of key controls and the overall cybersecurity program.

5. **Obtain independent assessment.** Well prepared organizations will challenge themselves with independent reviews and war game-type exercises. Bringing in external teams to play the role of the cyber-criminal can highlight vulnerabilities and mitigate confirmation bias. Additionally, there is a growing number of vendors that offer objective ratings and insights into a firm's cybersecurity risk profile, including review of a company's third-party vendors.

Cybersecurity is a complex problem that is not going to go away. To fulfill our fiduciary obligation, we need more than compliance or maturity model checklists. As fellow directors, we advocate a more quantitative, integrated, and value-based approach to help the board in assessing cybersecurity preparedness, risk mitigation and insurance strategies, and ultimately, the opportunities and risks of competing in the digital economy. 

Nate Fick is CEO of Endgame and an independent director of Strayer Education. James Lam is president of James Lam & Associates and an independent director of E*TRADE Financial. Shelley Leibowitz is a technology advisor and an independent director of E*TRADE Financial and Alliance Bernstein Holding.