MILLIMAN WHITE PAPER

# Translating cyber threats: How to communicate cyber risk in the boardroom

**Chris Harner**, FRM
**Chris Beck**

Milliman

During the Napoleonic campaign in Egypt, a French army officer made a startling discovery. While building Fort Julien in 1799, he noticed a slab with writing on it. The slab, now known as the Rosetta stone, provided a translation from hieroglyphics to Greek, finally deciphering ancient Egyptian writing. For many senior executives today, the jargon of cybersecurity may feel like hieroglyphics, a mysterious language that requires translation. There is a significant need in the market to transform cyber assessments, information technology (IT) metrics, and information security into the common language of risk management.

Furthermore, there is a lack of consensus on how to categorize cyber within a risk taxonomy. The insurance sector often views cyber as a financial risk, specifically a subset of insurance risk due to underwriting of policies. Banks may view cyber as a type of operational risk (i.e., people, processes, and systems) while other industries may see it altogether as a strategic or standalone risk. Assessing the effectiveness of a company's security protocols often falls short of assessing the more mature risks, such as credit and market. And no wonder: this very technical, high-velocity, and fast-evolving risk doesn't easily translate to any traditional metrics that board members typically are used to. This lack of a common vernacular creates a communication barrier between cybersecurity experts and the board. In order to bridge the gap, a new approach is required that makes it possible for stakeholders on both sides of the table to speak the same language.

## Look who's talking

To understand the cyber communication disconnect you have to first examine who's doing the talking. Most of the companies and technologies that power the interconnected world are barely old enough to drive—and even fewer are old enough to rent a car. The skills, tools, and language of the cyber professional are just as new. In contrast, the core skills and language of finance are well-tested and have been by the side of senior executives and board members throughout their careers. This communication relationship is akin to a teenager using emojis and text-message acronyms to communicate with someone who doesn't own a cell phone.

In today's cybersecurity and risk discussions, board members are often confronted with terms specific only to this risk, such as threat vectors, systems and applications, encryption protocols, phishing tests, password cadences, endpoint protections, and dozens of other inputs related to IT security. These cyber threats and controls are part of emerging concepts and language. Steeped in a vocabulary rooted in computer programming and IT systems, cybersecurity professionals often have backgrounds in coding and systems rather than finance, which can be a drawback in translating the details of a cyber vulnerability into the financial terms used to determine how to mitigate risk. Further complicating the situation is a class of "nontechnical" chief information security officers (CISOs) who are responsible for cybersecurity and reporting to the board, but who neither possess deep IT expertise nor rich content in risk management.

## High stakes

At this point, it may be important to digest what we just discussed, pause for a moment, and ask a critical question: Why should we care about translating complex technical language into financial terms? To cut to the chase: tens if not hundreds of millions of dollars could be at stake. Furthermore, if you are a CISO or chief risk officer (CRO) trying to communicate your cyber defense strategy, headcount and budget needs may be severely impacted.

Communication between cyber professionals and board members has been fractured for years because meetings are rarely held within the context of strategic decision making, e.g., consideration of risk appetite and tolerances, cost-benefit analyses, return on investment (ROI), operational outcomes, or other financial measures typically used by boards to weigh alternatives and prioritize initiatives. Consider the financial impact of a wrong decision—a mistake that came about because a disciplined methodology to effectively prioritize the initiative and weigh alternatives is lacking. In reality, many decisions related to cyber defense are similar to a fire drill. At first, some people delay in taking action, while some scatter; but without a holistic view and careful understanding of the actions that should be taken when someone yells fire, everybody runs. However, running during a fire is not as important as knowing where to run and planning the safest route in advance. As critical

as cybersecurity is, boardroom action on this issue is often reactionary or misallocated due to the difficulty in quantifying the risk, communicating the issues, and prioritizing action.

## Cyberattacks are adapting to change—risk models need to as well

Today, what passes for cyber risk assessment is really just another controls assessment. Controls exist to mitigate risk; cyber needs to shift to defining the risk and therefore from qualitative assessment to quantitative loss distribution. Finding a common language—a framework comparable to the one used for other risks—is further complicated by the unique nature of cyber risk. Unlike nearly every other risk, cyber's ever-changing nature stems from the fact that a human being is at the center of the attack, intentionally working to exploit a firm's vulnerabilities while outsmarting its defenses. And thanks to increasingly sophisticated and well-funded perpetrators, this can affect not only the types of attacks companies may experience but also the potential impact of a breach. Not only is the threat of cyberattacks changing rapidly, it often morphs and adapts faster than firms can keep up.

Moreover, as cyber threats have increased in sophistication, the attack surface is increasing the opportunity for exploitation. Today's wireless and interconnected ecosystems, which include a great many more players and devices than a closed operating system, provide even more opportunities to gain unauthorized access to systems or data. In addition, extended supply chains and multiple vendors expand the attack surface, complicating how to determine the actual threat and configure a comprehensive defense.

Meanwhile, the Internet of Things, the cloud, and other technologies continue to transform the processes and practices of businesses, making their functionality ever more interconnected and interdependent. The effects of one risk event (such as a partial system shutdown in operations) can weaken a management team's ability to respond to threats in other areas. New cyber risk frameworks need to be able to account for risks that influence each other, often in subtle but substantive ways that traditional, silo-based list management approaches are unable to identify and detect. Additionally, cyber data is not consistently captured while longstanding historical data does not exist for a risk that continues to evolve. Cyber models need to be able to balance industry data, company-specific data, assumptions, and expert judgment to avoid masking a risk that may have eluded traditional methods.

## Translating cyber into the same risk language

So how do you take the ever-changing nature of cyber risk and its technical components and translate it into traditional—and especially *actionable*—reporting metrics used in the boardroom?

An effective cyber risk model must measure, aggregate, and convert cyber metrics into intelligible reporting linked to the balance sheet, in particular how much capital is at risk in the event of a breach. This approach allows cyber risk to be reported in the same loss distribution framework as other risks. It also gives cyber professionals the metrics to convert a threat into an estimated loss and thus speak the board's language. From this vantage point, a company's board can decide how much cyber risk it is willing to accept and prioritize the implementation of cyber controls.

Cyber risk is the ultimate enterprise risk, impacting every part of the organization with numerous second-order and third-order effects—think reputational, strategic, and vendor risks, etc. Thus, cyber risk requires a new alignment between the CISO and the CRO—neither executive will succeed in achieving their goals to *protect the enterprise* if they cannot communicate effectively with the C-suite and board. With a holistic modeling capability for cyber risk, the CISO and CRO can tell a coherent story to senior management, allowing it to understand budgetary requirements, how to allocate funding more effectively, and how much capital is at risk due to a cyber threat, as with traditional risks.

The Rosetta stone provided the breakthrough needed to understand hieroglyphics and therefore the mysteries of ancient Egypt. Likewise, effective risk modeling will elevate the understanding of cyber risk to the level of traditional risks that the board and the C-suite are used to managing. An effective cyber risk model will translate the complexities of cyber defenses into actionable metrics, whether they're visuals, dashboards or other financial reporting tools. It's this shared language that can give board members and cyber professionals a jumping-off point to determine an acceptable level of risk, prioritize controls, and create actionable goals. Cyber risk is more than a threat—it is the ultimate enterprise risk. No cybersecurity program can fully insulate a business from attack. Rather, leadership must focus on how resilient its business is to attack. In order to understand enterprise resilience, the firm must acquire the capability to model and quantify cyber risk. With this capability, leadership can then make strategic and investment decisions with confidence on how to confront and mitigate the risk.

**CONTACT**

Chris Harner
chris.harner@milliman.com

Chris Beck
chris.beck@milliman.com