MARSH

Finding the Elusive Cyber Loss Curve Can Pay Big Dividends for Financial Institutions

What is the likelihood that your organization will experience a material cyber event in the next 12 months? Is the risk greater than 50%? Less than 25%? These questions are ever-present on the minds of risk managers, who long for at least a practical — if not precise — answer.

Cyber risks are among the most serious perils facing the financial industry. Cybercrime is not only increasing in frequency, but also in magnitude, costing the world an estimated $600 billion, or 0.8% of global GDP, according to a recent report published by McAfee and the Center for Strategic and International Studies. But while financial institutions have become practiced at estimating most operational risks and using this data to develop risk capital strategies, they often perceive roadblocks to extending these methods to cyber.

An Information Chasm

One major problem revolves around the lack of data. Unlike other risks, there is limited historical data about cybercrime, mainly because it is a relatively new risk area but also due to its constantly changing form. Cyber risk management has not yet been "reduced to practice" on a wide scale.

Traditionally, financial entities have used qualitative frameworks — red, yellow, green, or high, medium, low — to characterize cyber threats, a system also commonly used in other industries. This approach can be quite useful, but it is no longer sufficient for the financial sector, which has been feeling a growing need to put numbers to cyber risk, calculating both severity and likelihood. A more quantitative methodology is needed both to improve a company's protection and to comply with increasingly stringent regulations, including the Basel II framework and standards imposed by national regulators.

While this can be a complex endeavor, a starting point is to consider scenario analysis. This approach enables point-estimates of the financial cost — the *severity* — of cyber events with good accuracy. Significantly more difficult is determining the *likelihood* of an event. Having credible quantitative estimates for both severity and likelihood will allow risk managers to answer the fundamental question: "What is the likelihood that our organization will experience a cyber event causing a loss of greater than, say, $100 million in the next 12 months?" Most often, it is the *likelihood* question that derails many attempts at quantifying cyber risk, due to the unpredictable nature of a

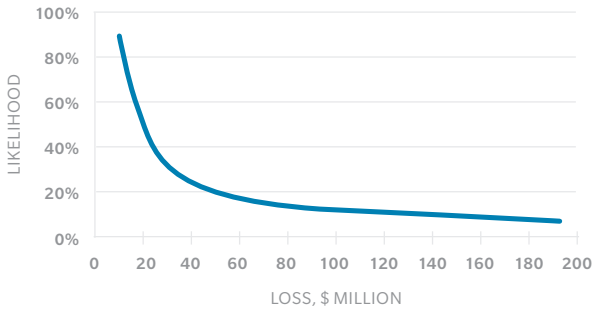
human-initiated threat. However, despite the limitations, financial risk professionals should enter this challenge holding to the adage that every risk can be modeled.

In recent years, driven by the Basel Committee on Banking Supervision's standards and guidelines, banking regulators both in the US and globally have emphasized the need for financial institutions to have adequate capital reserves by modeling a wide range of risks. Further, financial companies in the US are required to carry out stress tests on their balance sheets, looking at a number of high impact-low likelihood scenarios, including cyber events. And US bank examiners regularly carry out cybersecurity assessments of all banks.

In 2016, the Federal Reserve, the Comptroller of the Currency, and the Federal Deposit Insurance Corporation issued an *Advance Notice of Proposed Rule Making* (ANPR) declaring their intention to establish more stringent standards on systematically important institutions. Among other proposals, the ANPR asserted its aspiration to develop "consistent, repeatable methodology" to measure cyber risk. Its call for submissions for potential methodologies to quantify inherent and residual cyber risk underlines the necessity that the financial industry applies such procedures to meticulously measure cyber risk.

Beyond the regulatory push, there is high recognition within the industry that financial institutions must embark on robust efforts to identify and estimate cyber risk and protect their operations and customers from the disruptive and potentially costly repercussions of cyber-attacks.

FIGURE 1 Representative Loss Curve



Calculating the Loss Curve

When dealing with improbable events, *likelihood* and *impact* are inextricably linked; this is the case in every risk area. Generally, the relationship between the two can be expressed through a non-linear loss distribution curve (see Figure 1), which describes a situation where higher cost is associated with lower likelihood. Very costly events are rare; less costly events are more common. Where sufficient historical data is available, it can usually be described with this type of characteristic curve.

If a loss curve can be represented mathematically with a fair degree of confidence, it can open up tremendous opportunities for managing the risk it represents. It helps risk professionals calculate risk appetite and risk tolerance within their organizations, and to get a good understanding of the risks associated with events in the "tail" (the right side) of the curve. No model is perfect, but a data-driven estimate of the loss curve can enable business leaders to better understand the risks of cyber and take action to manage them.

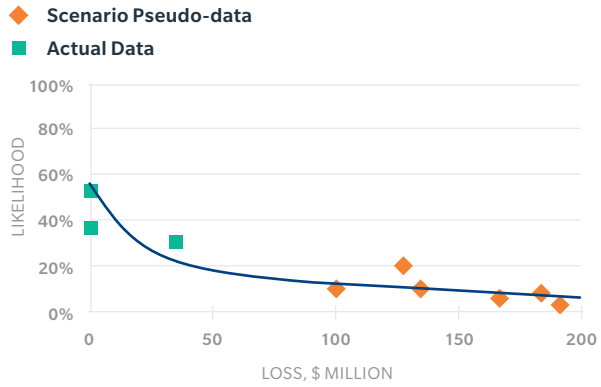
The loss curve has, in fact, been used as a backdrop for modeling operational risks for some time. But what about cyber? Cyber itself is, after all, an operational risk. Does the long-established loss curve idea apply to cyber? Certainly, the traditional loss curve has intuitive appeal when we think about cyber risk. It would seem that a loss of, say, $150 million due to a cyber-attack is at least somewhat less likely than a loss of $50 million. While there is no certainty that cyber risks can be described effectively with the traditional loss curve — could hackers cause *more expensive* tail events to become *more likely* than less costly events? — it is an attractive modeling approach to start with.

Developing a Cyber-Specific Loss Curve

Cyber is presently one of the most challenging among operational risks and it may be a long time, if ever, before there is sufficient historical data to develop an organization's cyber-specific loss curve with certainty. But scenario analysis can help. Risk professionals are already familiar with scenario modeling to sketch out the loss curve for operational risks. This approach can also work in cyber. A few simple rules apply to scenario development: focus on tail risks; aim for events that are unlikely but plausible; and ensure the events are organization- and system-specific with enough detail to analyze losses accurately. Once there are enough estimates for impact and likelihood, even with large confidence intervals, "pseudo-data points" can be plotted, and the loss curve starts taking shape.

The pseudo-data of scenario estimates can be combined with the actual data of real-world events, when these are available (see Figure 2). Through reasonable curve-fitting based on an assumed distribution — such as the log-normal, Poisson, or other — a financial institution can develop an approximation of the elusive loss curve for cyber.

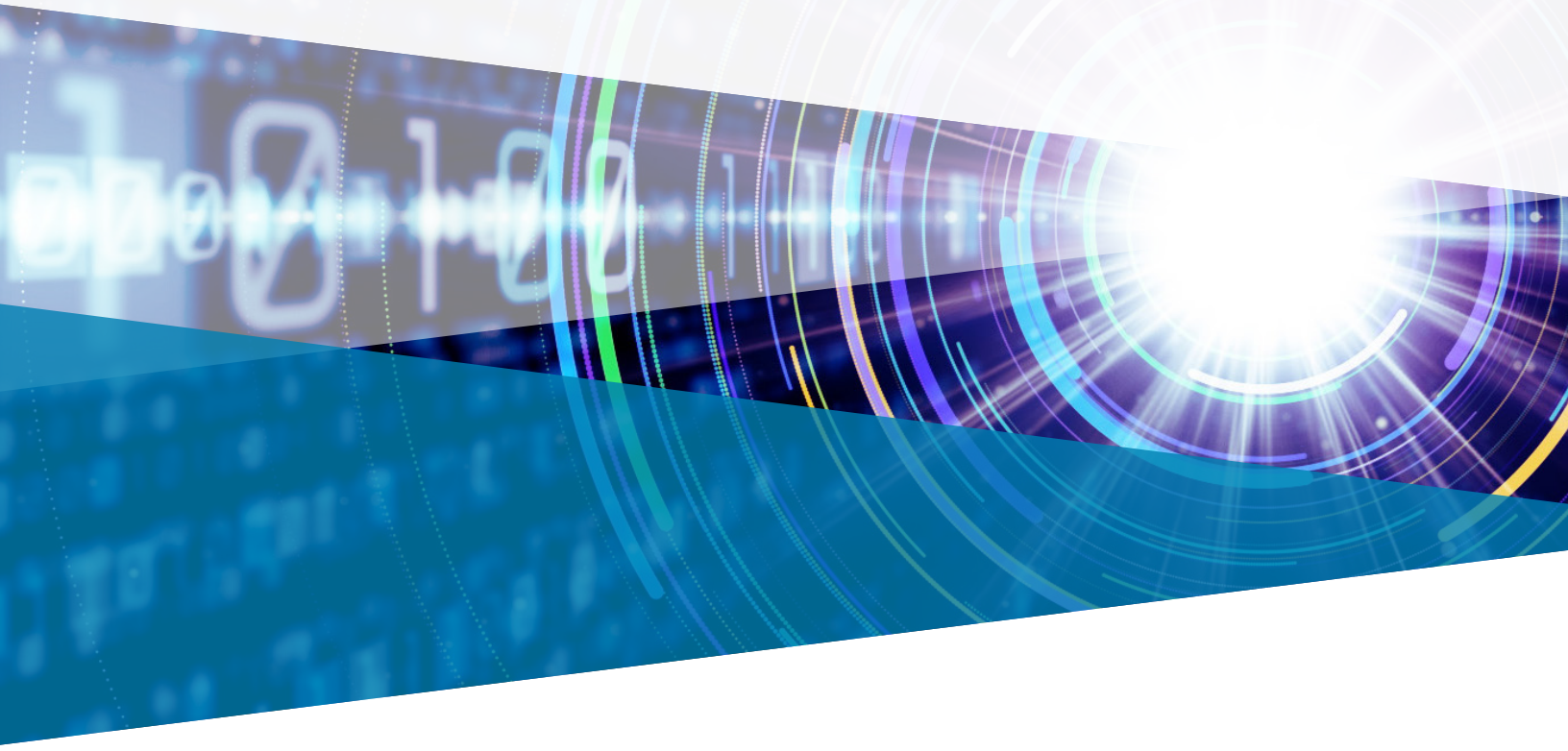
FIGURE 2 Blending Actual and Pseudo Data to Determine Cyber-Specific Loss



This type of analysis ties likelihood and severity together in a mathematical formula, offering insight for risk managers and other key figures into the risk that cyber poses to their organizations. Ultimately, finding the loss curve in cyber can pay big dividends. Financial institutions can use this type of modeling as an aid to developing a meaningful capital risk framework for cyber that can not only address regulatory requirements but also raise the organization's game in cyber risk management.

WHAT CYBER-ATTACK SCENARIOS SHOULD FINANCIAL INSTITUTIONS CONSIDER?

1. **Interruption or disruption of core banking platforms:** Identify the different areas that could be affected, and whether there could be alternative work practices that can be used during a down period.
2. **Corruption of databases:** Consider whether you need to have physical copies to continue operations in case of a cyber-attack.
3. **Corruption of back office systems:** Determine the cost of such an interruption and create a robust backup plan.
4. **Interruption of electronic trading platforms:** Brokers, investment banks, exchanges, and others involved in buying and selling of stocks, bonds, and other financial instruments should look at whether they can operate with lost or degraded connectivity.
5. **Extended internet service disruption:** Determine how your institution will be affected if you, and others that you do business with, are forced offline for an unspecified period of time. Consider whether some, or all, operations can continue offline.



For more information, visit marsh.com, contact your Marsh representative, or contact:

THOMAS FUHRMAN
Managing Director
Cybersecurity Consulting and
Advisory Services
Marsh Risk Consulting
thomas.fuhrman@marsh.com

ALEX DELARICHELIERE
Managing Director
US Banking and Capital Markets
Industry Leader
Marsh
alex.delaricheliere@marsh.com

KEVIN L. RICHARDS
Managing Director
Global Head, Cyber Risk Consulting
Marsh Risk Consulting
kevin.richards@marsh.com