Deloitte.

A framework for quantifying cyber risk: Pipedream or possible?

By integrating data into your risk assessment models, you can create a common vernacular to empower your organization to devise risk-intelligent responses to cyber threats.

For financial services organizations, cybersecurity is about much more than meeting regulatory mandates. Ultimately, it's about trust. Boards, executives, and the organization at large recognize their fiduciary responsibilities to customers—and take those duties seriously.

Yet, when it comes to identifying cyber risks and efficiently allocating resources towards mitigating them, the industry continues to struggle. Certainly, many financial services organizations have taken steps to identify the risk scenarios most likely to affect them and have modelled the financial impacts should those scenarios come to pass.

But are the numbers accurate? Can they be relied upon when making significant cybersecurity investment decisions? And what about the scenarios they can't predict? Let's face it: threat actors are ingeniously creative. Recently, one of the largest cybersecurity insurance providers in the US suffered a breach of its own, potentially positioning the hackers to target already-insured companies—and introducing yet another novel attack vector.[1] How can businesses calculate, and plan for, this type of variability?

An evolving approach designed to help organizations proactively assess these hidden risks is cyber risk quantification. Leveraging advanced modeling techniques, cyber risk quantification uses quantification models to estimate the range of probabilities and impacts of potential security events so that leaders can calculate key financial risk metrics, such as value at risk or expected loss. The concept is to apply a well-designed model to specific use cases so that you can estimate impacts and loss probabilities, determine a loss distribution, and calculate dollar loss metrics.[2]

It's cutting-edge. It's critically needed. The only problem? It's not quite ready to stand on its own.

[1] Cyberscoop, March 24, 2021. "Top insurer CAN disconnects systems after cyberattack," by Tim Starks. https://www.cyberscoop.com/cna-cyber-insurance-breach/

[2] Deloitte. "Beneath the surface of a cyberattack: Collision avoidance." https://www2.deloitte.com/us/en/pages/risk/articles/quantifying-cyber-risk-to-chart-a-more-secure-future.html

By ensuring everyone agrees on your organization's highest relative risks, it becomes easier to gain consensus on which controls are most relevant, which gaps must be closed, and which investments are critical.

A new model for cyber risk

Taking a quantitative financial approach to cybersecurity risk management is certainly a compelling idea. Applying hard numbers to risk scoring could help (Chief Information Security Officers (CISOs) and Chief Risk Officers (CROs) strengthen their business cases and bolster risk management, both on a day-to-day basis and in preparation for a potential future breach. It's also a capability that may ultimately play a central role in the world of cyber measurement.

Yet, in the interim, financial services organizations still need a repeatable framework to determine how risks emerge and where best to allocate their resources. They're simply unlikely to succeed if they continue relying on a static governance and investment process that inadequately acknowledges the dynamic nature of cyber threats.

One of the main challenges is that the cyber landscape changes often and quickly. Just as soon as companies identify their critical assets, risks, and mitigating controls, the targets shift—the risk envelope widens, the regulatory environment evolves, and new maturity gaps yawn open.

Equally as challenging is the fact that cyber events typically unfold in unpredictable ways. For every 'above the surface' cost organizations can identify in advance, there are myriad 'below the surface' impacts that are hidden from view. It's this identification of constantly-shifting, and often invisible, variables that current quantification approaches can help with.

Diving deeper

Cyber risk quantification has similarities to sports analytics which involves using data and statistical models to augment intuition and experience when developing a game strategy. Many sports have specific, well-known measures; when combined with quantitative analysis there is an opportunity to bring another perspective.

Cyber risk quantification works in much the same way. An additional measure is to review the controls you have in place, assessing which are (or are not) effective, and identifying control gaps. When augmented with cyber risk quantification, you have another dimension to guide cyber investment decisions.

From there, you can start to layer in additional context. For instance, while you may not be able to financially quantify the likelihood of black swan events, CRQ can give you unprecedented visibility into their potential impacts. This can help you pinpoint which risks may be relatively higher than others, and which might generate high impacts even if they are less likely to occur.

This insight, in turn, empowers you to choose how to respond. By integrating this data into your risk assessment models, you can create a common vernacular across your three lines of defense. With a consistent language and framework, both executives and the board will be better able to devise risk-intelligent responses—whether that means bolstering your controls, allocating additional resources, or mitigating through a cyber insurance policy.

The result is deceptively simple: By ensuring everyone agrees on your organization's highest relative risks, it becomes easier to gain consensus on which controls are most relevant, which gaps must be closed, and which investments are critical.

Power through knowledge

Although quantifying cyber risks from a dollar and cents perspective is still evolving, cyber risk quantification can help organizations identify hidden costs, gain visibility into most likely scenarios, and begin tracking the currently-opaque rippling aftereffects of a cyberattack. The value of this insight should not be underestimated. By shining a light into previously shadowed corners, cyber risk quantification gives financial services organizations a decision-making rubric—empowering you to more effectively steer your investment decisions and inform your budget spend.

Authors and contacts

Nick Seaver | Global Cyber Financial Services Industry Leader

nseaver@deloitte.co.uk

Mark Nicholson | US Cyber Financial Services Industry Leader

manicholson@deloitte.com

John Gelinne | US Cyber Managing Director

jgelinne@deloitte.com

Daniel Soo| US Cyber Principal

dsoo@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see http://www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.