The benefits and limits of cyber value-at-risk

Jacques Buith
Managing Partner
Clients & Industries Leader
for Global Risk Advisory
Deloitte Netherlands

Dana Spataru
Senior Manager
Risk Services
Deloitte Netherlands

The World Economic Forum's Partnering for Cyber Resilience initiative developed a preliminary framework for a statistical model which CIOs and other executives can use to begin quantifying the financial impact of cyber threats.

Many CIOs across industries struggle to answer questions about cyber risk posed by their executive teams and boards of directors: How likely are we to experience a damaging attack? How effective are our existing risk mitigation measures? If we spend US$20 million more on cyber risk mitigation, how much would that reduce our risk?

In the interest of helping organizations answer these and other questions, members of the World Economic Forum's Partnering for Cyber Resilience initiative recently proposed a working model for measuring and quantifying the impact of and exposure to cyber threats. Known as cyber value-at-risk, the model provides a starting point for quantifying risk and attempts to inject more discipline into that process, although it requires further refinement and field-testing.

With a goal of allowing corporate leaders to quantify more of the cyber risks their organizations face at a more granular level, cyber value-at-risk ultimately seeks to help them make more informed, confident decisions about their organization's risk tolerances and thresholds, cyber security investments, and other risk mitigation and transfer strategies.

Despite the current challenges in applying the model, companies that have been exposed to cyber value-at-risk express enthusiasm for it. One organization working with the World Economic Forum's cyber resilience initiative obtained a more structured view of its risk profile by using the model, and now the organization is making more fact-based security investments and policy decisions as a result.

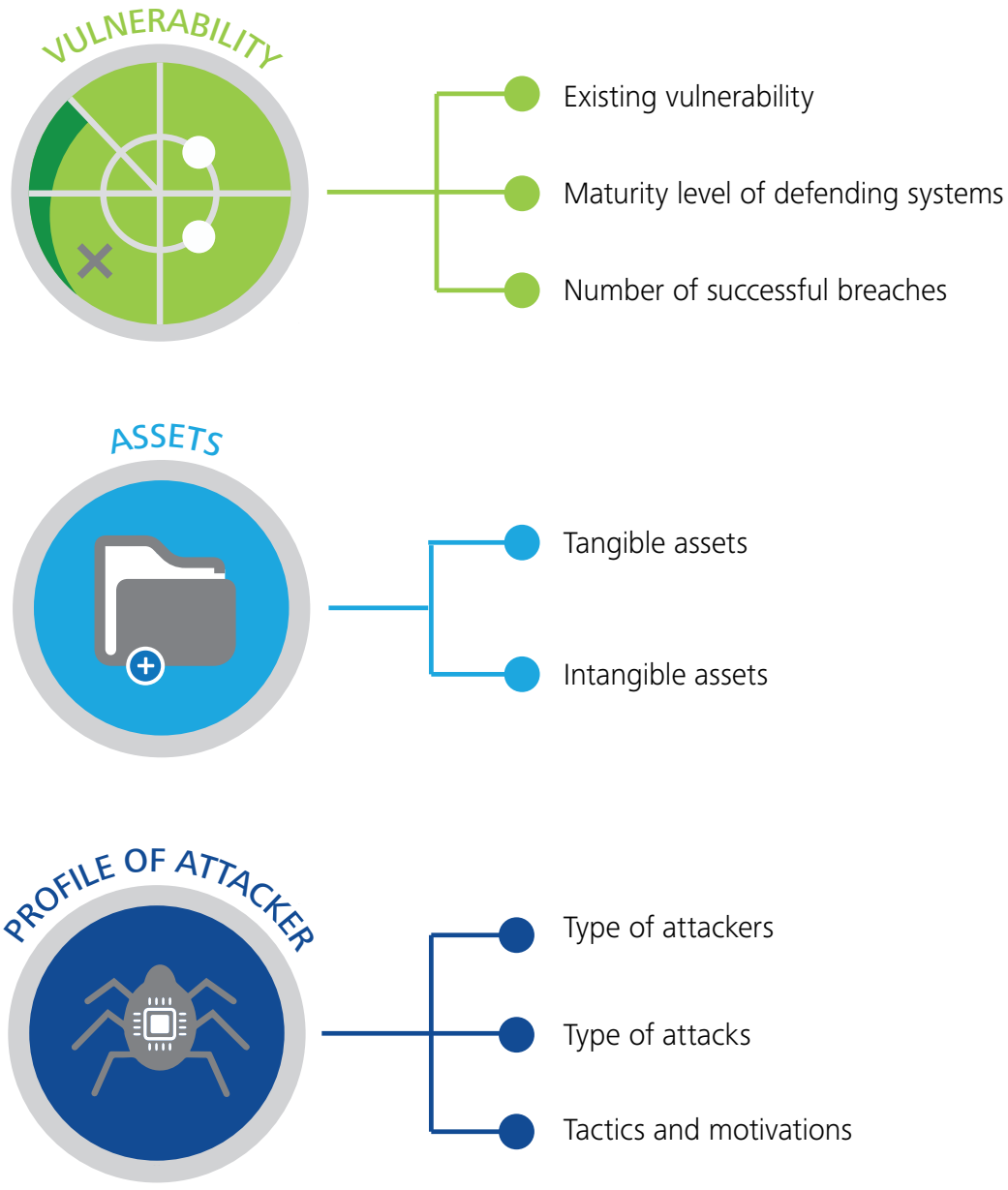
The roots and components of cyber value-at-risk

The concept of cyber value-at-risk is based on the notion of Value-at-Risk (VaR), a statistical technique widely used in the financial services industry to express a bank's level of financial risk (or the financial risk associated with a specific investment portfolio) over a specific period of time. Similarly, cyber value-at-risk seeks to use probabilities to estimate likely losses from cyber attacks during a given time frame.

Cyber value-at-risk considers three primary drivers, or components, of cyber risk for an organization: its vulnerability, its assets, and the profile of its potential attackers. Analyzing dependencies among the three components is critical to estimating risk exposure using cyber value-at-risk. For example, the number of attacks a company is likely to experience largely depends on the value of its assets to potential attackers and trends in the attacker community. Therefore, the company's assets and the attacker profile determine the extent to which the company may be a cyber-attack target.

Cyber value-at-risk considers three primary drivers, or components, of cyber risk for an organization: its vulnerability, its assets, and the profile of its potential attackers

Figure 1: Cyber value-at-risk components



Source: World Economic Forum, "Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats"

One of the biggest challenges associated with obtaining accurate results from cyber value-at-risk is the ability to estimate the probability of a successful attack

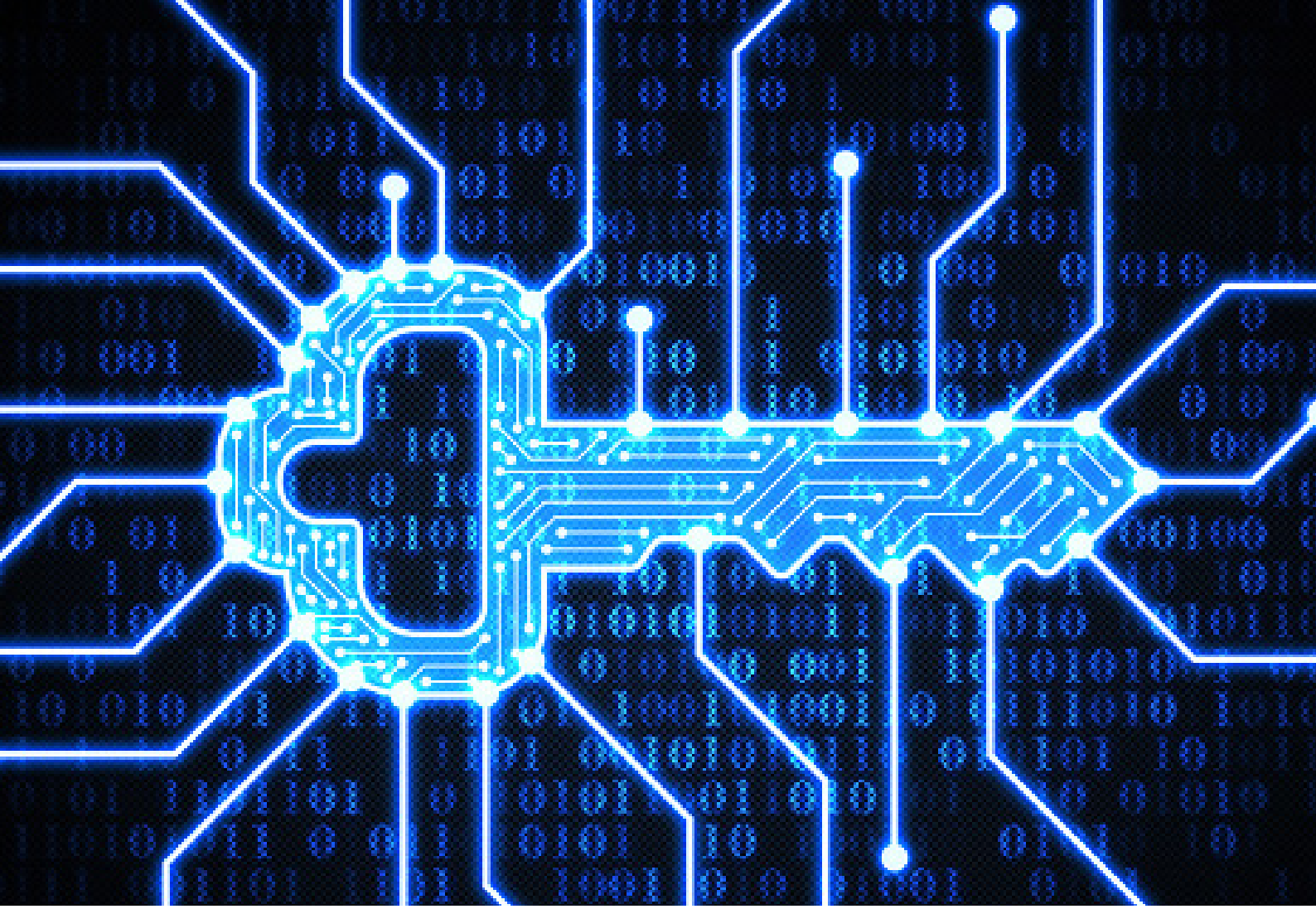
Vulnerabilities take into consideration, for example, the number of unpatched systems inside an organization, the number of previous compromises it has experienced, and the maturity level of its defending systems as defined by the number of security updates applied, the number of defensive software components installed on the network, and the network typology and infrastructure.

Assets vary by organization, but on the tangible side, they typically include funds and financial instruments, infrastructure, production facilities, and financial losses incurred through temporary business disruption, complete business interruption, and regulatory fines. On the intangible side, assets frequently encompass intellectual property (IP), customer or employee data, and a company's reputation.

Attacker profile looks at the type of attackers, whether they are amateurs, state-sponsored, or part of organized crime rings; their motivations (e.g., financial gain, theft of trade secrets, destruction, reputation damage); and the sophistication of the attacks they tend to perpetrate.

The limitations of cyber value-at-risk

One of the biggest challenges associated with obtaining accurate results from cyber value-at-risk is the ability to estimate the probability of a successful attack. Doing so requires a large set of real-world historical data regarding the frequency and severity of risk events that is not yet widely available, for the reasons that follow. Obtaining reliable cyber risk data is hindered in part by delays between the time cyber events occur and when organizations detect (and report) them. Given that current regulations in the United States require reporting on only a subset of cyber attacks, the availability of data to understand, for example, attacker behavior is likely to remain limited until a broader culture of cross-industry and public/private sector information sharing takes shape. (Some of these regulations include the Health Insurance Portability and Accountability Act's breach notification rule and various states' security breach notification laws.)



Furthermore, the range of possible vulnerabilities an attacker may exploit may not be perfectly quantifiable: software vulnerabilities sometimes remain unidentified for years; dependencies on third-party infrastructure may limit visibility into the status of various assets; and the ability to anticipate future or evolving attacker motivations is an imperfect science. The degree of complexity and rate of change in many environments will continue to require an emphasis on establishing vigilance to detect the unexpected and resilience programs to support business recovery when a successful attack does occur.

The lack of standard maturity frameworks also limits cyber value-at-risk's current effectiveness. The number of incidents an organization is likely to experience depends in part on its relative cyber maturity, but without a standard maturity measure applicable across industries, quantifying threat "attractiveness" remains more subjective than objective.

Finally, cyber value-at-risk supports only a limited number of risk scenarios at this time. The probability and impact of outlier incidents, like an attacker stealing a waste management company's credentials to a client's systems in order to compromise the client's network, remain difficult to determine using cyber value-at-risk.

The future of cyber value-at-risk

It took the financial services industry 30 years to refine value-at-risk to the point where it is useful and trustworthy. Honing cyber value-at-risk will also take time, but those who invested in the model are working diligently to craft a usable version.

With a conceptual framework for cyber value-at-risk established, a next step is applying real-world data to the model. Our hope is that exposing the potential benefits of cyber value-at-risk will prompt industry participants to share more of the data needed to make the model work effectively. In the meantime, CIOs can use the notion of risk-based quantification to position themselves to use the cyber value-at-risk model and justify budget requests to the executive team and board.

Printed with permission by Deloitte Netherlands