WHITE PAPER

Cyber Value at Risk: Quantify the Financial Impact of Cyber Risk

Bay Dynamics®

Contents

Bay Dynamics®

Bay Dynamics Application Value at Risk Enables Enterprises To Prioritize Cyber Security Activities In Real Time Based On Potential Financial Loss

No matter how many resources at their fingertips, cyber security experts consistently struggle to keep up with the overwhelming amount of threats and vulnerabilities standing in their way. Cyber security is a hectic grind with tens of thousands of security events cropping up across hundreds of different applications each day. Each of these applications usually run with numerous open vulnerabilities waiting for fixes. And, typically, more than a few users who tap into these applications engage in some sort of risky behavior that needs to be curtailed.

There's never enough time in the day to address all of these problems, so effective cyber security depends on effective prioritization. Ideally, that prioritization should be indexed against dollars and cents.

Organizations should be taking the timeliest action against cyber risks that are likely to be the costliest to the business. Sounds simple enough. But this is hardly a simple or an ideal world.

The truth is that until now there has been no straightforward way to track specific security threats, vulnerabilities or user actions against the financial impact to the organization. Most organizations today are flying blind when it comes to tying security actions and investments to financial risk. As a result, cyber security remains a practice of gut instinct and fuzzy statistics — messy, expensive and ineffective.

If enterprises are to take their cyber risk programs to the next level, they need to be able to translate cyber security into the language of financial impact. This takes discipline and the right technology to establish the practical application of a business metric called Value at Risk.

Cyber security and Value at Risk

Value at Risk may be unfamiliar to many technologists, but it is hardly a new concept in the business world. It's a long-standing business metric for financial and operational risk management. Fundamentally, Value at Risk measures the intersection of the likelihood of an event happening and the potential financial loss if that event happens.

It has been used for years in everything from insurance to financial modeling. In a cyber security context, Value at Risk can be used to measure the financial impact to the business if an application were compromised, and prioritize mitigation actions based on that metric. The threats and vulnerabilities that, if exploited, would cause the most financial damage to the company should be the ones enterprises tackle first.

Enterprises and the security industry have long recognized the importance of bringing greater quantitative discipline to cyber security, and many have attempted to calculate potential financial losses in some form or another. So far, attempts have fallen short.

For example, the roughest estimates depend on generalized benchmarks like the Ponemon Cost of Data Breach statistics compared against high level valuations of customer data or intellectual property. These are the kind of FUD statistics that may scare boards into spending more on the overall security budget but do nothing to direct how it's allocated on a strategic or operational level, and ultimately come back to haunt CISOs when at the next meeting they cannot consistently quantify improvements/decline of the same metric.

Meanwhile, some companies have created quantitative models that calculate Value at Risk based upon security experts guesstimating the value of the asset and probability of loss. These estimates may be based on a point-in-time snapshot of internal data or on the small amount of general statistical data available in the industry. While the algorithm is scientific, the inputs are based on estimates, not actual conditions on the ground. As any computer programmer will tell you, garbage in, garbage out.

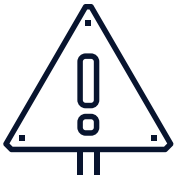
Not only are the numbers from this method imprecise, but this type of Value at Risk calculation also suffers from another major shortcoming. Namely that they're typically made on a yearly or quarterly basis. Requiring significant human intervention and constant inputs, it just isn't feasible to constantly update the calculation. So even if the estimates were entirely accurate and precise, the Value at Risk calculation made with this method is a single-point-in-time measure. It's still not a consistent metric upon which security teams can base their day-to-day decisions.

With all of these weaknesses, those in the cyber security industry have largely viewed accurate Value at Risk as a bit of a unicorn measure. It's perceived as impossible to achieve due to a historical lack of accurate data and understanding of how that data contributes to the measure.

However, that is changing. Moving forward, enterprises will find that they can come to a serviceable cyber security Value at Risk calculation if they can meaningfully put together the following elements:

Inventory
Accurate IT asset inventory

Asset Value
IT asset value estimates



Vulnerability Scoring
Accurate and timely list of existing vulnerabilities in all assets ranked by criticality

User Monitoring
Real-time telemetry about user behavior in relation to cyber security policies

SOC Data
Security event data from the IT environment, such as indicators of attack/ compromise

Solid Algorithms
A platform that weaves in analytics built with the understanding of the interaction between all these variables

Putting these elements together requires a technological anchor in the heart of cyber activities, something that can continuously monitor for the main risk factors that could cause big losses. It also requires data science expertise to develop the quantitative framework that will automatically come up with continuously measured Value at Risk based on a continuous feed of security data.

Since the Bay Dynamics Risk Fabric® platform collects, correlates and analyzes threats and vulnerabilities that put enterprises' most valued assets at risk of a compromise, the platform already contains the essential ingredients for calculating a reliable Value at Risk metric.

Bay Dynamics Risk Fabric Application Value at Risk

Bay Dynamics' Risk Fabric cyber risk analytics software continuously monitors the enterprise environment and collects all the necessary data to compute a realistic potential for exposure. The platform gathers loss impact information and puts all the pieces together to compute the Value at Risk metric.

Risk Fabric bakes in an advanced calculation for application-level Value at Risk. Called "Application Value at Risk", this risk scenario analyzer is the first of its kind because it is calculated daily and it is based on actual telemetry data from the enterprise security and IT environment.

This is no periodic point-in-time calculation based on subjective probability estimates from users or security staff. It's a reliable metric that will help executives get a handle on the financial impact of potential events. With this in hand, they can finally establish a cyber risk program that prioritizes remediation based on value and validates how much risk was removed from the business due to actions taken.

At its simplest, Application Value at Risk is a calculation comprised of three major variables: **Application Credential Exploit Potential, Application Technical Exploit Potential** and **Application Total Loss Potential:**

$$\text{Application Value at Risk} = f\left[\begin{array}{l}\text{Application Credential Exploit Potential,}\\ \text{Application Technical Exploit Potential}\end{array}\right] \times \left[\begin{array}{l}\text{Application Total}\\ \text{Loss Potential}\end{array}\right]$$

Here's a rundown of how data for each of the major variables is collected and parsed.

Application Credential Exploit Potential

Whether it is through a compromised account or a user inside the company who is breaking policy for malicious or careless reasons, credential-based issues are a prime vector for potential exploits. Risk Fabric calculates this composite number based on authentication events to and from each application's hosts.

Application Technical Exploit Potential

Malware and other automated software-based threats are the other key vector for potential exploits. Risk Fabric scores this variable based on endpoint events (indicators of attack/compromise) to and from the application hosts, as well as on the vulnerability posture of the application.

Application Total Loss Potential

An estimate of the asset value provides the foundation for assigning a dollar value to the potential financial loss from losing confidentiality, integrity or availability of an application. Application Value at Risk also provides the option of either 't-shirt' sizing estimates or more detailed estimates provided by application owners about the relative value and security requirements of an application. This will be done through Risk Fabric's easy-to-use Application Owner Questionnaire.

Putting Application Value at Risk to Work

With all of this environmental data in hand, the underlying algorithms developed by Bay Dynamics' data scientists calculate the aggregate potential for exploit of any given application and multiply it against the financial loss potential supplied by the customer. The result is a dollar figure estimate that provides a tangible way to understand the financial impact of cyber risk based on actual threats and vulnerabilities in the enterprise's environment.

This Value at Risk metric provides an extremely valuable translation layer to communicate cyber risk across the business. With it in place, there are a number of key ways that enterprises can elevate their cyber risk programs.

Remediation ROI Measurements

Risk Fabric provides a value for any given remediation effort by estimating the decrease in Application Value at Risk once a vulnerability or threat is addressed. The platform then ranks vulnerabilities with the highest return, offering a truly disciplined means to prioritize operational activities.

CSO Strategic Decisions

With Application Value at Risk in hand, CSOs and other risk professionals will be able to make more informed decisions about how to run their organizations and allocate resources. In the past, it has been difficult for cyber risk professionals to make apples to apples comparisons of the impact of vulnerability management programs against threat mitigation programs and so on. Remediation ROI measurements allow leaders to compare effectiveness based on financial impact.

Using Risk Fabric, CSOs and risk leaders can now conduct 'what if' scenarios to identify optimal actions that align their organizations' cyber risk with their board's risk tolerance. The system also provides 'recommended actions' that enable risk professionals to reach their goals based on remediating specific threats and vulnerabilities in their environment.

More Informed Cybersecurity Investment Decisions

Additionally, cyber risk professionals now have a valuable tool for engaging with the board and CEO. Not only can they offer the board meaningful updates on Value at Risk improvements over time to justify their efforts, but they can also drill down into the data to offer targeted suggestions for future investments by aligning the allocation of budgetary dollars with business impact and the best cyber security ROI.

About Bay Dynamics®

Bay Dynamics® enables enterprises to continuously quantify the financial impact of cyber risk based on actual conditions detected in their environment. The company's flagship product, Risk Fabric®, is a software platform that calculates the value at risk associated with specific threats and vulnerabilities, that when mitigated, measurably reduce cyber risk exposure. Using Risk Fabric, stakeholders across the business can prioritize their remediation activities and direct their limited resources at the risks that matter most. Risk Fabric benefits enterprises with a financial measurement of cyber risk that's based on current detectable conditions in the enterprise environment, gathered from existing security tools and business context. The platform also provides value based prioritization of remediation, reduced regulatory risk, reduced costs and improved timeliness of action by automating the delivery of personalized and prioritized vulnerabilities to line-of-business application owners responsible for remediation. For more information, please visit www.baydynamics.com.