CSCMP hottopics

SEPTEMBER | 2019

Supply Chain Security: How to improve digital resiliency

Joshua Berg, Cybeta

In an increasingly interconnected world, it is more important than ever to evaluate the digital resiliency of an enterprise – the capability to withstand and operate right through a cyber threat or a verified incident. Digital resilience processes ensure that an organization's infrastructure and services can operate with minimal disruption during a cyber threat or incident. Unfortunately, modern digital networks are rarely built with resilience in mind.

To build digital resiliency, an organization needs to:

1. Gain support from the board and senior leaders, who can ensure that cybersecurity considerations are included at all levels of strategic decision-making, and support changes in culture and mindset. Responsibility and accountability for cyber resilience sits with these executives
2. Change the mindset from reactive to proactive resilience, embedding cybersecurity into the everyday choices of end-users
3. Build strong cyber defense into business processes and information technology systems, taking into account the organization's entire digital footprint
4. Identify reliable tools to measure and track resilience, replacing the trial-and-error or low oversight approach that has traditionally been the default for many organizations.

In a typical large corporate network there are countless devices, including ones from multiple vendors operating both independently for specific functions and integrated with each other for seamless cross-system operations. To assess resiliency, operators need an overview of the network in its entirety, rather than just examining separate segments. Operators need diagnostics, intelligence, and the capability of threat modeling to make changes to logical controls, access management, and supply chain network security in an efficient, prioritized and repeatable manner.

When risk and information security managers approach a CFO with budget requests to build more resiliency within the enterprise network, the CFO will likely ask how the organization will know that the plan is working, and will want reassurance that the team will not need a further budget increase the next year. The challenge with quantifying the risk is equally present in quantifying the benefit of additional investment in technology, security upgrades or both.

Cybeta™ offers a proprietary, statistically proven tool, Threat Beta™, which offers the reassurance that operators and CFOs need to build a digitally resilient organization. Threat Beta is a comparative metric that quantifies cybersecurity vulnerability, threat vectors, and attack likelihood. As part of a layered defense, this is indispensable to accurately identify critical attack vectors and direct resources towards attack prevention. Cybeta's proprietary methods include three primary analytic modules: Threat Surface (how big are you on the Internet?), Weighted Vulnerability (relative vulnerability with technologies analyzed in context), and Attack Likelihood.

CSCMP™

Educating and Connecting the World's Supply Chain Professionals.™

Armed with Threat Beta, companies measure their cybersecurity posture from an attacker's point of view and get instant metrics comparing their environment to global attack trends and patterns. In combination, this allows companies to be given a contextualized comparison to the real, verifiable and quantifiable hacker activity occurring globally and the statistically weighted probability of a future breach. In simple language, the higher your company's Threat Beta rating, the more likely it is that an attacker will exploit your vulnerabilities.

We have taken a range of complex characteristics and boiled them down to a Threat Beta metric. Threat Beta mimics financial beta and is pegged to a scale of 0-2. This global metric and proven predictive indicator helps evaluate potential outcomes and provides a practical framework for discussing these outcomes with boards and other senior executives.

Consider an example where your enterprise network has a Threat Beta score of 0.66, which indicates an overall cyber risk 34% less than a comparable statistical subset of entities. As part of normal business growth, you assess the network of an organization that your company plans to acquire and see a Threat Beta metric of 1.67, representing a substantially higher risk than both your own firm and the average firm globally. By connecting to the other company's network, your organization's inherited risk would rise, an outcome either wholly unacceptable or requiring significant unplanned financial investment to improve their security. However, if you decide to proceed with the acquisition, you could use this information to renegotiate the price and add new liability escrow elements.

As a strategic element in building an information security program, Threat Beta is mostly used on a day-to-day basis by operational leaders, who are making ongoing changes to the network. As an example, Threat Beta is used by an international manufacturing firm to gauge their internal priorities and monitor and alert their vendor security team about critical, actionable intelligence related to any of the hundreds of vendors that they label as being business-critical.

The Threat Beta metric is used to understand critical issues, changes in posture over time and adherence to contractually mandated security. A service level agreement is in place for the provider to bring the network up to certain levels over specified periods of time. Supply chain companies can use this tool to understand whether these network changes are getting better or worse.

By measuring cyber-attack probability against technologies, this tool provides a predictive analysis of where future attacks are likely to occur. This analysis prevents attacks before they happen because it provides a holistic picture of the threat risk and helps companies make an informed assessment of where a cyber-attack could occur.

Threat Beta can help you confidently track your organization's digital resiliency on a daily basis, boosting compliance and improving incident response.

ABOUT CYBETA™

Founded in 2019, Cybeta™ offers a suite of Cybersecurity products and services designed to help you keep your business off the Cyber 'X'. Based on decades of detecting and thwarting the activities of even the most advanced attackers, Cybeta™ delivers the substantive intelligence you need to make preemptive strategic and operational decisions. Think in terms of over-the-horizon visibility coupled with enhanced peripheral vision.

About CSCMP Hot Topics

Issues of *CSCMP Hot Topics* may include early results from ongoing research being conducted for CSCMP or other organizations; new supply chain practices, thought-provoking ideas, or emerging trends; discussions of changes in the broader business and regulatory environment that may impact the supply chain and logistics field.

CSCMP

Educating and Connecting the World's Supply Chain Professionals.™