Visualizing Cyber Risk: Defining Business Priorities for Remediation

Published: August 2016 **Report Number:** A0257

Analyst: Dr. Alea Fairchild, Entrepreneur-in-Residence

Share This Report

What You Need To Know

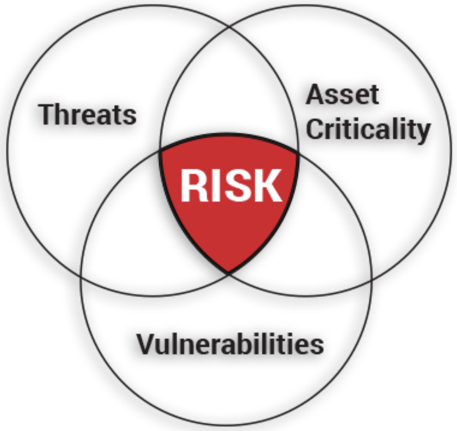
Enterprises continue to find it a challenge to address vulnerabilities and susceptibilities to risk for the business on a wider scale. Although most enterprises employ a variety of cyber security tools and policies, many lack the visibility and cadence (or rhythm) to program and/or leverage a holistic organizational approach to risk and vulnerability. This can impact the timing of patches and prioritization of remediation based on the severity of risk and criticality to business operations, reducing both time to mediation and future damage costs. Although we would like to be *proactive* and engaged on risk management, we end up being *reactive,* with security tools used in a restricted manner based on audit requirements; with no clear view of the attack surface or what has been exploited.

AT A GLANCE

This report examines the business drivers for a more holistic way of looking at cyber risk. There is an urgent need to be able to focus more clearly on root causes, susceptibilities, and actions that are relevant to critical business operations.

What we really need is the ability to orchestrate remediation and quickly monitor the results. How can we better visualize cyber risk as to understand our systemic susceptibility and its relevance to the business? Let's start by defining cyber risk, and why understanding our risk profile and being able to visualize a risk baseline is optimal for timely decision-making and resource allocation to be able to focus on the applications that provide information critical to customer experiences.

Defining Cyber Risk



What is cyber risk? How does it differ from cyber security? The concepts are not interchangeable, as securing IT assets is not the same thing as knowing the risk that the inability to utilize an asset has on the business. Cyber risk is a macro view of operations with a wider business-specific focus and relevance at the intercept of threats, vulnerabilities and asset value.

On the financial side, organizations are already familiar with risk frameworks (SANS, COBIT) where IT risk is subjectively controlled. But we believe cyber risk goes beyond a control framework and constitutes an overview of the hygiene / well-being of the potential attack surface of the organization. Without a proper risk surface definition, it is difficult to find the root cause(s) of an attack and to proactively do a susceptibility analysis of the IT assets. What is needed is the ability to unify and contextualize internal security intelligence, external threat data, and business criticality across the growing attack surface of the enterprise—which is more than just the network!—including applications, devices, and IoT.

Defining the role and extent of cyber risk in business operations in today's environment is important, not only for the Board in terms of compliance and governance, but also for the IT team in understanding the business criticality of IT assets and prioritization for remediation efforts. This is why having a visual tool that aggregates and analyzes the data for both sets of stakeholder is important for risk mediation. In speaking with a financial services solution provider for this research, they stressed the importance of categorizing risk as the business sees it.

Why Cyber Risk Impacts the Business

Business priorities have to matter in how the assets are secured and managed. Cyber risk is both temporal and topical, where both vulnerabilities and stakeholders matter. The ecosystem that manages remediation must do so on a risk-based prioritization of threats. This is where management of risk goes from human interaction to human-interactive machine learning, as the risk scoring needs to be cleanly in line with business objectives, and geared to measure and manage in that light. Without putting vulnerabilities into the context of the risk associated with them, organizations often misalign their remediation resources.

> “He who defends everything defends nothing.”
>
> **Frederick the Great**
> *(Frederick II of Prussia)*

Viewing Cyber Risk in a Susceptibility Model

One way to view how to manage cyber risk is in a similar way to the SIR model in global health. In SIR models, the flows go between three states: susceptible (S), infected (I), and resistant (R). In cyber risk, we can use a modified version:

S – Susceptibility of the attack surface and how it is maintained;

I – Infection and infiltration levels / state of the system(s)

R – Recovery state, with remediation analysis and the underwriting of sustainability of this state

In visually modeling the attack surface with a remediation tool that orchestrates the state of the system, its infection level, and the hygiene of the attack surface, teams can shorten time to remediation and increase operational efficiency by (for example) assigning tickets for triggering pre-defined workflows.

So what is holding enterprises back from analyzing their cyber risk profile in a SIR model? It is two-fold: the security tools used for gathering information are not well-automated, and the effort to access, aggregate, and analyze the information is not fully integrated. Our research shows that existing problems integrating security tools to analyze cyber risk are caused by the following obstacles:

- Manual data aggregation and analysis: Causes slowness of response and visibility.
- Lack of context for remediation: Causes resources to be allocated inefficiently as a function of impact.
- Lack of prioritization for mitigation, with no rating or scoring for priorities: Causes resources to be committed to less critical functions.

In examining the need for scoring, Blue Hill has been talking to users of the RiskSense Platform, which offers its RiskSense Security Scoring (RS$^{3)}$ scoring system. This enables the IT team to decide what is the most mission-critical remediation, and what resources should be allocated to what problem(s) as and when they occur. It also maps vulnerabilities to corresponding controls and compliance findings.

> “RiskSense helps us prioritize what we should be working on.”
>
> *CISO*
> *Fortune 200 Telecom Company*

Insightful Ways to Visualize Threats

How can their visual approach help? Visualization allows teams to view the orchestration, and to see the wider picture, tied to business objectives and business risk. Nelnet.net, one of the organizations we interviewed for our research, talked about the efforts they took previously to integrate data entered manually into vulnerability management tools, and their need for visualization in managing complex dimensions of risk in an integrated platform.

For them, RiskSense integrated the data from a variety of sources on vulnerability management vendors. They not only automated the data analysis, they enriched it visually so Nelnet.net could see the business criticality to focus remediation actions on the things that mattered to their organization.

Cyber Risk: Observations and Recommendations

Cyber security has been pushed as a concept by the need for compliance, data breaches, regulatory audits, and legal ramifications. Although many companies are working hard to address cyber security, one of the challenges is that IT departments have a hard time articulating their cyber risk profile and the relevance of certain systemic vulnerabilities to the business operations. What enterprises need to do is try to address their susceptibility to cyber risk, specifically focusing on root causes, being able to clearly define the attack surface and articulating how vulnerable business critical operations are on the basis of the criticality of the business function.

> “RiskSense easily sets the important information in front of the resources needed to remediate.”
>
> **Ryan Regnier**
> *IT Director*
> *Nelnet.net, USA*

For your cyber risk strategy, Blue Hill recommends that your enterprise:

- ✓ **Understands your cyber risk**: understand what information really matters, what types of risk you care about and how exposed you are;
- ✓ **Sets strategic priorities** to ensure your risk mitigation enables growth; make sure that risk controls also enable progress; and that you remain agile enough to re-examine processes based on risk profiling; and
- ✓ By using visualization tools, **makes an active decision on risk**: set your risk appetite, communicate it to all functions and ensure your resources are effectively deployed. Visualize your risk in a way that sets clear priorities on the utilization of resources.

Blue Hill's research suggests that the RiskSense Platform, with its orchestration and visualization tools, should provide a standout differentiator for organizations that take the time to consider these factors in their evaluations. Visualization of application attack path analysis allows firms to visualize and remediate the most critical vulnerabilities on the basis of the risk to the business. In a world where trillions of dollars are susceptible to cyber risk, organizations and enterprises of all sizes must be able to view cyber risk to be more cost-efficient and proactive in their remediation and management of their risk profile.

ABOUT THE AUTHOR

Dr. Alea Fairchild

Entrepreneur-in-Residence

Dr. Alea Fairchild is an Entrepreneur-in-Residence at Blue Hill Research. Alea covers the convergence of technology in the cloud, mobile, and social spaces, and helps global enterprises understand the competitive marketplace and to profit from digital process redesign. She has expertise in the following industries: industrial automation, computer/networking, telecom, financial services, media, transport logistics, and manufacturing. Her clients are both commercial, government / public sector, NGO and trade associations. Dr. Fairchild received her Ph.D in Applied Economics from Limburgs Universitair Centrum (now Univ. Hasselt) in Belgium, in banking and technology. She has a Masters degree in International Management from Boston University/Vrije Universiteit Brussel, Brussels, Belgium, and a Bachelors degree in Business Management and Marketing from Cornell University. She is a masters Olympic weightlifter for Belgium, having won many international medals.

Connect on Social Media

@AFairch

linkedin.com/in/aleafairchild

bluehillresearch.com/author/alea-fairchild

For further information or questions, please contact us:

Phone: +1 (617) 624-3400
Fax: +1 (617) 367-4210

Twitter: @BlueHillBoston
LinkedIn: linkedin.com/company/blue-hill-research
Contact Research: research@bluehillresearch.com

Blue Hill Research offers independent research and advisory services for the enterprise technology market. Our domain expertise helps **end users** procure the right technologies to optimize business outcomes, **technology vendors** design product and marketing strategy to achieve greater client value, and **private investors** to conduct due diligence and make better informed investments.