CyberProof™

SHALL WE TELL THE BOARD?

GAINING CLARITY AROUND CYBER RISK AND INVESTMENT

YOU KNOW HOW MUCH YOU'VE BEEN SPENDING ON CYBER SECURITY. BUT DO YOU REALLY KNOW HOW EFFECTIVE YOUR INVESTMENT HAS BEEN?

How well do you understand your current risk exposure? Do you believe your cyber spending improved this posture? As it turns out, few executives can answer these questions with any sense of certainty. Let's see why.

ASSESSING YOUR RISK POSTURE

Our understanding of cyber security risk tends to be based on information received from news sites, blogs, vendors promising they will protectus, and a thin monitoring layer in your SOC normally designed to meet regulatory requirements. The result? Enterprises spent too much money, time and effort firefighting, meeting regulatory requirements and installing breach prevention tools.

As described by John Giordani in this article in Forbes, the concept of risk for cyber security is incredibly complex. And with ever-increasing threats and a shifting IT landscape, enterprises need a deeper understanding of their risk posture and their ability to respond.

The purpose of risk measurement is not to quantify the exact "value at risk" but rather to drive the right behaviors – in terms of where organizations spend money and invest time and effort.

IT'S SHIFTING SANDS

We're facing ongoing changes to threats such as new exploits and zero-day malware. And at the same time, we have a more complex IT environment. Once, everything was behind a firewall, but now the surface area includes mobile, the Cloud, the Internet of Things - exponentially harder to protect.

New threats crop up daily: According to the AV-TEST Institute, over 350,000 new malware (malicious programs) and PUA (potentially unwanted applications) are registered every day. Moreover, according to VirusTotal, between 300,000 and 500,000 distinct files are detected by one or more search engines every day.

The only way forward involves "zero trust" - meaning, an organization cannot trust anything inside or outside its perimeters and it must go through a verification process before it grants any access. When the starting point is "zero trust," it becomes essential to obtain all possible event data - to evaluate everything and only then, to analyze alerts.

To manage this much information, it is important to understand the most important cyber security risks and prioritize accordingly. Looking at risk the way an insurance company evaluates risk means understanding cyber risk events. Like a hurricane, a cyber event has an estimated "magnitude of loss" and an "event frequency." Starting with the cyber events that pose a high "Value at Risk" to the business allows cyber security teams to prioritize assets, detection, prevention, and response to these event scenarios - making spend more efficient.

WHEN BUSINESS PRIORITIES DRIVE SECURITY SPEND

An old aphorism commonly attributed to the statistician George Box is, "All models are wrong - but some are useful."

At CyberProof, we approach risk modeling using a top-down model where the key question is: What are the primary threats to your business? A top-down approach defining the magnitude of attack and focusing on the top two to three attack scenarios is critical to making it practical.

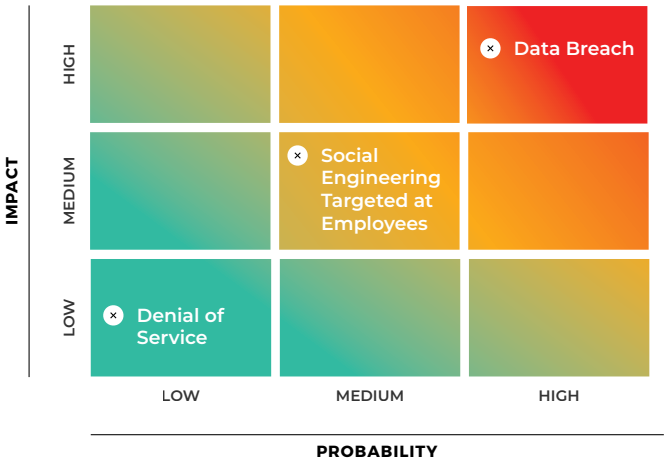

Figure 1: Focusing on the top two to three attack scenarios

Based on that information, we facilitate a business-oriented prioritization of your investment in defense and response.

To ensure you spend optimally, we break down risk into distinct categories:

1. Pre-breach - is what you can do before a breach-ensuring you have the right technologies to protect yourself, manage vulnerabilities, and track a constantly morphing threat environment.

2. Post-breach – is what you do ahead of time to prepare for an attack - identify how to detect, respond, and recover faster so as to lessen the impact on your business, operations, and reputation.

Enhanced Event Monitoring
Advanced correlations leveraging native integrations with number of security tools and platforms

Human Driven Advanced Threat Intel
Targeted threat intelligence, data analytics supplemented by expert human driven intelligence

Collaborative Incident Handling
ChatOps based collaboration for collective incidenthandling, isolation and faster issue resolution

Continuous Vulnerability Intelligence
Enhance traditional vulnerability tools utilizing continual breach simulations and control validation

Accelerated Incident Response
Automate low level tasks and incident response playbooks as well as centralized incident response processes

Figure 2: Reduce cyber risk to the right level for your business

PEN TESTS AND RED TEAMING ARE NOT ENOUGH

Vulnerability testing is another classic example of where traditional approaches are insufficient. Typically, organizations conduct a quarterly penetration test and an annual red teaming exercise - and come up with a list of fixes.

But daily pressure to release code to production and constant changes in IT environments means that vulnerabilities show up every day. Even with the most expensive security protection, hackers simply wait and exploit a vulnerability or a mistake.

For red teaming, although it's an exercise designed to see how an advanced attacker might penetrate a target, it's still manual; it must only find a single path to its target. There could be many paths, and typically - there are.

In today's threat environment, companies require continuous vulnerability monitoring using a complete set of advanced hacking techniques performed on the highest priority targets. Speedis the name of the game.

Continuous Visibility

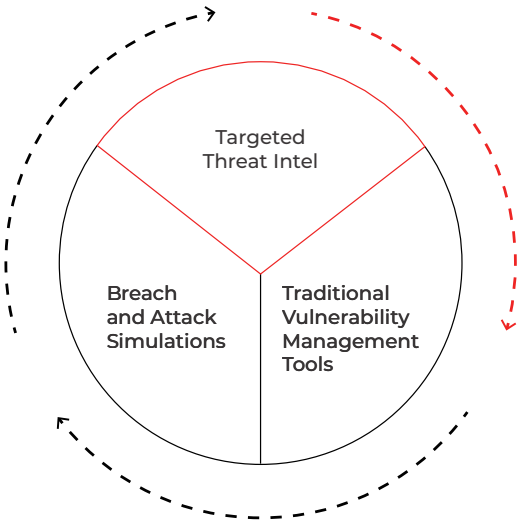

Figure 3: Obtaining a comprehensive view of vulnerability risks

To do this cost-effectively requires awareness regarding business priorities in terms of risk - the ability to rank activities based on the potential business impact of an attack. For example, let's say IT is installing a patch on a thousand servers, the team must know which server should be patched first.

THE ROLE OF MANAGED SECURITY SERVICES

Boards of major companies are generally aware that it's impossible to guarantee there won't be an attack - no matter how much an organization invests. Boards are also well versed in assessing financial or regulatory risk. The problem is that cyber risk is generally not well understood and, as a consequence, an accurate assessment of cyber risk is poorly communicated to the board.

The real question is whether we're putting in enough time and focusing the right resources to make sure we reduce the risk of the most important attacks - and are prepared to detect, respond, and recover from an attack as quickly as possible. Meeting this challenge requires enhanced technical and procedural competencies that most organizations don't have. And that's where managed security services come in.

Increasingly, CEOs are finding value in services that augment the skills of their in-house staff with flexible, on-demand cyber security expertise - that works with an organization to reduce the probability that a vulnerability in a critical system will turn into a major event.

For the next generation of Managed Security Providers, the major impact areas are (1) the continuous ability to find and mitigate vulnerabilities in critical systems, (2) the ability to proactively predict threats, especially targeted attacks, (3) the ability to detect key attack tactics and methods in critical systems, and (4) the ability to respond effectively - reducing the possibility of an attack turning into an event or successfully managing a high profile event.

DIGITAL HYGIENE KEEPS THE BAD GUYS AWAY

In our complex IT environment, most hackers count on the human factor - waiting for people to make a simple mistake such as clicking on a link, making a configuration error, or failing to patch an application server. Hackers must only find one mistake - whereas defenders must avoid all mistakes. Most companies focus on patch management, but the problem is actually far more complex.

Let's say, for example, an admin adds a file with write permissions on the default login directory. It's a small, administrative mistake - simply forgetting to change the default from "write permissions" to "read only." But it opens up everything. There's no tool out there that can protect you from this kind of error, which hackers exploit to get in.

CyberProof has partnered with XM Cyber to create XMProof. The joint solution conducts extensive "purple teaming" - continuous vulnerability testing that uncovers these kinds of errors - i.e., both by searching for the vulnerabilities ("red teaming") and by suggesting the remediation ("blue teaming").

This type of breach and attack simulation has become essential because, with the amount of change happening every day, mistakes certainly are going to be made.

Lowering risk requires focusing on the right things. For most, it means placing less of the focus on prevention solutions - and more on basic digital hygiene and maintaining actionable situational awareness.

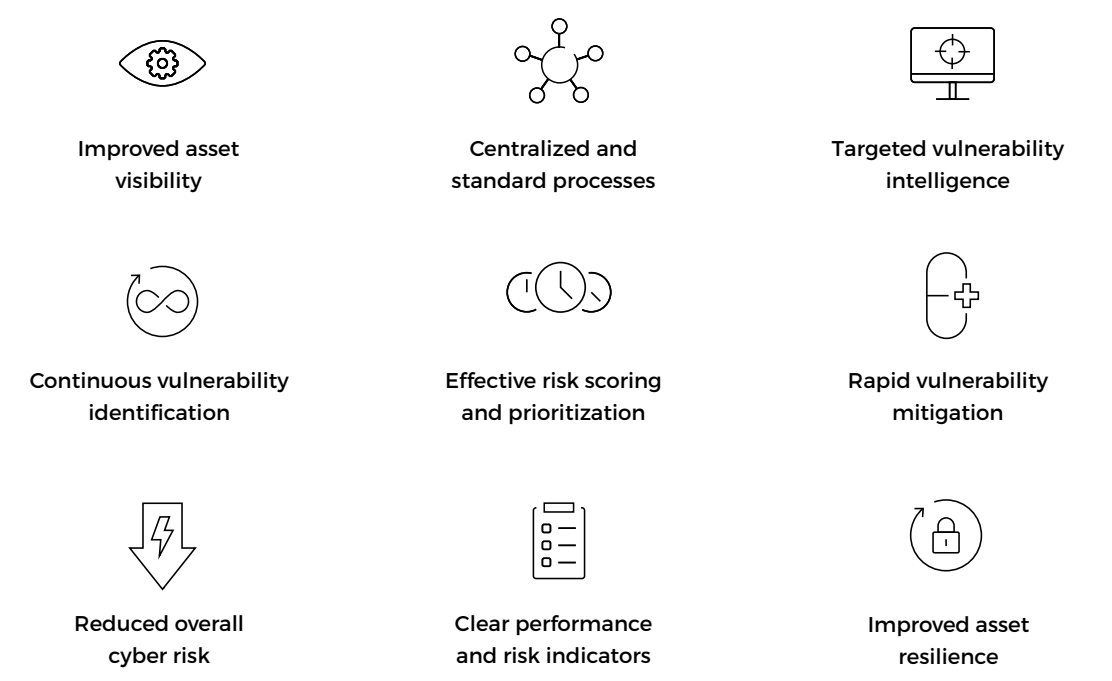

Figure 4: Converting cyber risk into measurable outcomes

SPEAKING ABOUT BUSINESS RISK WITH FAIR

One of the challenges today is that conversations with the CEO and board tend to be too technical. Boards and CEOs are well versed in supporting effective decision-making, but to do this - they need to have the tools to assess an organization's potential loss exposure or value at risk.

At CyberProof, we leverage the FAIR risk model to simplify the risk equation, making it practical to measure value at risk as a business risk conversation - i.e., geopolitical risk, regulatory risk, etc. Cyber risk, however, needs to be tracked on a continuous basis.

FAIR is the only internationally recognized, risk-based approach to information security and operational risk.

Using the FAIR model, one can define an equation that relates to (1) Magnitude of Loss for the Risk ($), and (2) the Frequency of Event. In other words, start out by defining the magnitude of loss for the top two or three risk scenarios. This should be an annual type of consulting assignment that defines critical risks - from 50,000 feet down to the threat actors, key assets, and priority vulnerabilities - and that measures the impact of remediation and ROI.

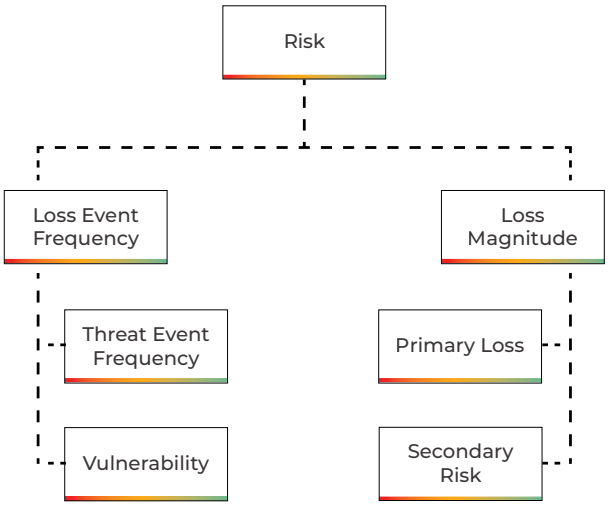

Figure 5: Assessing loss exposure in financial terms

We abstract Threat Event Frequency to focus on what matters. For the top two or three risk scenarios, the Threat Event Frequency is always rated as high or very high. For large enterprises, for example, the highest risk might be disruption of critical client networks or exfiltration of valuable client data. The actual frequency may be initially assumed based on FAIR guidelines and later validated based on the number of detected alerts against defined systems.

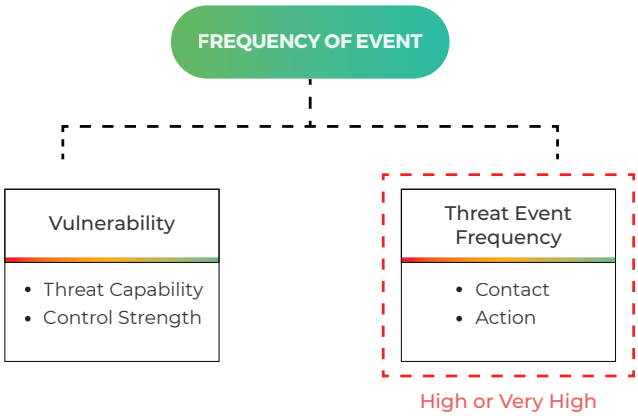

Figure 6: Abstracting Threat Event Frequency

We focus on the vulnerability calculation by leveraging XMProof to understand the "threat capability" against a defined system, and by leveraging the CyberProof Defense Center to understand the "control strength" from detection through response.

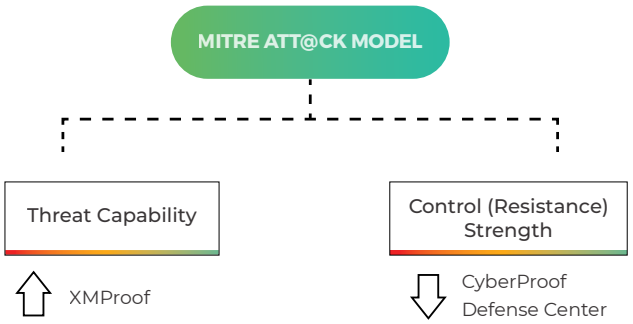

Figure 7: Leveraging XMProof and the CyberProof Defense Center

RISK-BASED PREMIUMS

Boards are willing to pay more where they see value in terms of risk. Though the current MSSP market has been commoditized as they race toward the lowest price - price is not necessarily the determining factor for the board, when it comes to security.

At CyberProof, we believe risk drops dramatically when an organization improves its risk level as compared to its peers in the industry. This ties into the work of insurance companies, who find it easier and cheaper to provide insurance for companies with lower risk.

There is an inflection point at the industry level - a striking shift in risk when you get a little better, as compared to other players.

For example, let's say a hacker is looking to steal healthcare records. Hackers go for easiest targets. If I'm the easiest in my industry to hack, I'll get hacked first; but if I'm better protected than other players, I'm significantly less likely to be hacked.

Thus, a risk-based approach opens the door to partnerships with insurance companies. According to Josephine Wolff in Wired, insurance companies may consider providing discounts if a company's risk level is maintained by a recognized external service, within the bounds of a defined risk zone.

WHAT IF YOU PAY FOR A CYBER RISK OUTCOME?

Executives complain that the old managed security service providers provides little value, that the legacy MSSP industry is broken. In fact, the industry has been focused (for too long!) - on meeting regulatory requirements. To move into a new mode that provides optimum value, the business model must change.

Imagine this: What if you could present cyber security in terms of Value at Risk on a continuous basis to your board? What if you could quickly correlate a new threat in terms of "value at risk" to your business?

Cyber security risks and vulnerabilities are changing on a daily basis. Imagine something indicating a drop or rise in value at risk, like a stock price fluctuates based on events of the day. The only difference is that the value of risk should trend downward not upwards like the stock price.

The value is based on both pre-breach risk (how well you manage vulnerabilities) and post-breach risk (how well you are prepared for critical attack scenarios). When the next global attack is discovered, the board can get a clear risk score of the organization's risk level. It's also clear when risk levels return to "normal" - to a business risk profile appropriate for the organization.

With this ongoing knowledge of business risk, perhaps the CEO will have the kind of insight necessary to focus on the things that really keep you safe from serious attacks. Perhaps a decision will be made to invest a little more and drop risk levels to better protect your brand. Perhaps insurance companies will offer a cyber insurance plan that meets the needs of the business.

Pricing cyber security services based on value at risk, as proposed by CyberProof, revolutionizes the conversation with your board. It provides a disruptive model in the industry based on effectively maintaining risk levels - giving you optimal value from every dollar of security spend.

ABOUT CYBERPROOF

CyberProof, a fully owned subsidiary of UST Global, is a platform-enabled company, whose mission is to reduce cyber risk with flexible service models. At CyberProof, we approach risk modelling using a top-down model where we define the magnitude of attack and focus on the top attack scenarios. We then facilitate a business-oriented prioritization of a customer's investment in defense and response.

CyberProof was recently ranked Leader in the Forrester Wave™ Report: Emerging MSSPs Q3 2018, validating our disruptive approach to cyber security services.

For further information visit www.cyberproof.com.

LOCATIONS

Boston | Trivandrum | Madrid | Tel Aviv | Aliso Viejo | London