Cyberint

MANAGING CYBER RISK EXPOSURE

HOW TO ACT WHEN YOU CAN'T MEASURE CYBER RISK

It's difficult to manage what you can't measure – and unfortunately, measuring cyber risk exposure can be a serious challenge.

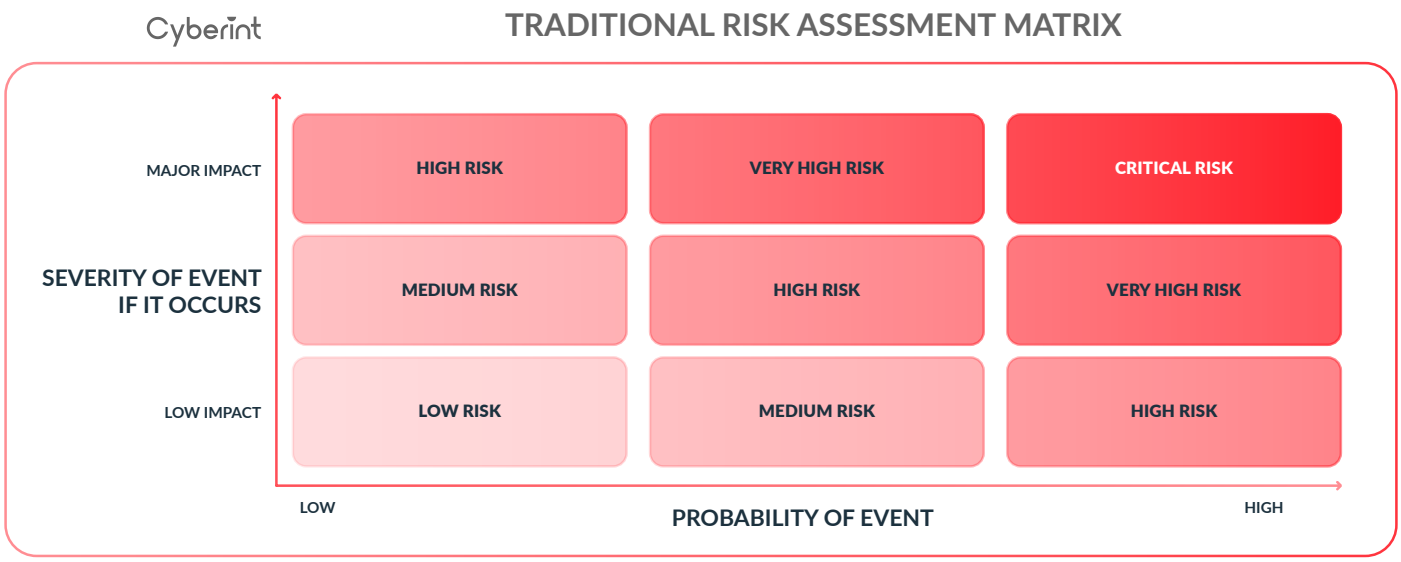
This short ebook will discuss challenges with measuring risk and provide strategic guidance on how to plan your security program in the absence of a reliable mechanism for quantifying risk.

Challenges With Measuring Cyber Risk

Most organizations have a great deal of trouble with measuring and labeling various cyber risk factors. This is not for lack of trying. In fact, there is a great deal of effort placed on identifying, quantifying, and deciding how to manage cyber risk.

For instance, virtually every vulnerability database, including the NIST NVD, include severity ratings via CVSS designed to help organizations determine just how much of a risk each vulnerability poses. In another example, most threat intelligence feeds assign a confidence level to every indicator of every compromise (IoC) on a scale from 0 to 100 to inform consumers of how likely a particular IoC is to represent a real risk.

In general, organizations attempt to categorize cyber risk using matrices that look something like this:



There are a few major limitations that arise from this approach. For starters, it's very difficult to accurately estimate the probability of an event, even with plentiful data and information available. Similarly, predicting the severity of an event before it occurs is also very challenging. When push comes to shove, an event that you estimated to be low impact may turn out to have an extremely significant impact. After all, hindsight is 20/20.

Moreover, the InfoSec community currently lacks standardization in cyber risk assessment. There is no common unit of measurement to quantify the severity of a risk or event. Various organizations will define different events in different ways. For instance, one organization may reserve the term "security incident" for only very severe events, whereas another organization may count very minor occurrences as "security incidents."

Making Do With Imperfect Information

The reality is that risk management is rarely as neat and tidy as scoring systems imply. The same risk may affect different organizations in different ways. Depending on the types of IT environments you operate and how they are configured, a risk that might be severe for one organization may turn out not to pose any threat to you, or vice versa.

Plus, risks can change in real time, and they are affected by many variables. Leaked employee credentials that appear on the Dark Web may not be a big deal initially. But they can become a very serious risk if a ransomware operator purchases them.

Cyber risk assessment is further complicated by the fact that it's very difficult to place a dollar amount on a risk. You might know, for instance, that a phishing website that impersonates your brand will have a negative financial impact on your business, but exactly how much it will cost is hard to say. It's even harder to forecast how risk costs might change if threat actors deploy additional phishing sites or expand their attack to other vectors.

You can make predictions, but until an attack is in the rear-view mirror, you can never achieve anything approaching a reliable calculation of the cost of a risk.

In short, cyber security risk analysis is almost never comprehensive or scientific. The best you can hope to do is validate that a risk is real, then make informed estimations about how serious the risk is likely to be.

Responding to Cyber Risk

Just because you can't perfectly measure cyber risk exposure doesn't mean you can't manage it. When faced with a risk, you can respond in one of the four ways: avoid, mitigate, transfer, and/or accept.

Avoid

Avoidance means stopping whatever exposes you to the risk. If you discover that a specific type of software is vulnerable, for example, you can simply find a more secure alternative.

The obvious downside here is that shutting down resources may disrupt business operations. But it also prevents the exploitation of risks, so it's a viable strategy in situations where you believe the risk is truly severe and you can foresee no other mitigation measures.

Mitigate

In cases where you know how to mitigate the risk, that's usually preferable to avoidance. Risk mitigation means taking a certain action – such as patching a software product after a new vulnerability is discovered – that minimizes the chances of attackers exploiting a risk.

Mitigation doesn't necessarily fully eliminate risks. For instance, if you update the credentials of a compromised account, there's a chance that the method threat actors used to compromise the account remains viable, and that they'll simply steal the updated credentials, too. But in many cases, mitigation is an effective means of rooting out risk.

Transfer

Another cyber risk management strategy is to transfer the risk to someone else. You could, for example, purchase cybersecurity insurance, which won't prevent threat actors from exploiting vulnerabilities but will at least reduce the financial fallout of a breach, if one does occur.

Transferring risk is often reserved for risks that cannot be avoided or adequately mitigated. You don't really solve the root problem, but you insulate your business against the risk.

Accept

A fourth option is to accept the risk and do nothing to address it. This makes sense when you do not believe the risk is severe and the time and effort required to mitigate it outweigh the benefits of remediation.

In this scenario, it's still important for the security team to document the risk, including estimations on the potential financial impact of this risk, and share the findings with senior leadership. If the organization's leadership decides to accept the risk, they must sign off on the documentation to accept responsibility for the fallout if that particular risk leads to a costly incident.

Choosing the Best Cyber Risk Mitigation Strategy

Of these four options, mitigation is almost always the best course of action. The other three approaches – avoidance, transfer and acceptance – either don't remove the threat or, in the case of avoidance, are likely to have a negative business impact due to operational disruptions. Additionally, cyber insurance providers have both raised premiums and implemented stringent requirements for new organizations to procure an insurance policy, so transferring risk must always be accompanied by mitigation actions.

Now, choosing to avoid, transfer or accept a risk might make sense if you could reliably measure each risk. But as we explained above, you can't. Just because you think a risk is minor enough to accept, for example, doesn't mean it actually is – and if you miscalculate, you could end up deciding to ignore a risk that turns out to have severe consequences.

The bottom line: Whenever possible, mitigate risk.

Cyber Risk Mitigation Strategies

How do you go about mitigating cyber risks? The answer depends, of course, on factors like the nature of each risk and the resources available to you. But in all cases, risk mitigation should reflect the following approaches.

Cyber Threat Intelligence

Threat Intelligence underpins many other critical aspects of cybersecurity, from network security and IAM to vulnerability management and governance, risk and compliance. Gain strategic, operational, and tactical threat intelligence to optimize all aspects of your security program.

Attack Surface Management

Continuously discover and monitor your Internet-facing assets for vulnerabilities, misconfigurations, and other common security issues. This helps you to identify and remediate potential attack vectors before bad actors find and try to exploit them.

Brand Protection

Proactively search for impersonation of your brand on lookalike domains, phishing sites, social media platforms, app stores, and more. Monitor social channels for impersonation of your organization's executive leadership team.

Deep & Dark Web Monitoring

Gain visibility into hidden forums and marketplaces on the deep and dark web where threat actors plan their attacks. Detect threats like data leaks, exposed credentials, and malware infections, as early in the cyber kill chain as possible.

Digital Supply Chain Security

Continuously monitor your vendors, suppliers, and partners for major cyber risks. COmprehensively assess their security posture using open, deep and dark web data. Receive a real-time alert when a 3rd party is attacked or breached so you can protect your organization.

A Comprehensive Approach to Cyber Risk Management

Seasoned InfoSec professionals understand that cyber risk measurement is always a "best effort" activity. Nobody expects cyber risk to be quantified with perfect accuracy or consistency.

Nonetheless, businesses must be aware of risks and prepare to act strategically whenever new risks arise. Ideally, that means:

- gaining a robust understanding of the risks that an organization faces
- assessing the severity of each risk as accurately as possible
- deciding which risk management techniques to employ for each risk
- mitigating cyber risks to the greatest extent possible, given other constraints

By mapping out your organization's external attack surface and delivering comprehensive intelligence collected across the open, deep, and dark web, Cyberint can help you every step of the way as you optimize your cyber risk management program.

Request a free deep and dark scan from Cyberint to check our Intel Data Lake for threats like exposed credentials, data leakage, malware infections, and more.

CLAIM YOUR ASSESSMENT NOW

Why Customers Choose Cyberint

"Because we're a small team, the Cyberint analysts are like an extension of us, which really helps from a risk management standpoint."

Evans Duvall, Cyber Security Engineer, Terex

Read more in the customer case study.

"We realized that Cyberint was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web."

Benjamin Bachmann, Head of Group Information Security, Ströer

Read more in the customer case study.

About Cyberint

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.