BlueVoyant

The Perfect Score:

Key Scoring Requirements for Measuring Third-Party Risk

Today's CISOs are tasked with the challenge of allocating limited funds and resources to focus on high priority cyber security projects, ranging from breach detection to response. Shortages in budget and skills require security leaders to make critical decisions or compromises when it comes to implementing a cohesive cybersecurity strategy. And with the average total cost of a data breach being $3.92 million in 2019, it's not surprising that most of that money is spent on protecting their own network.

But what about protecting their assets from risks posed by third-party relationships?

Nowadays, it's pretty much impossible to find a company that doesn't utilize third-party vendors.

In a recent report, the Ponemon Institute found that 63% of respondent companies experienced a data breach caused by a third-party or vendor.

Solutions like BlueVoyant's 3rd Party Cyber Risk Services can help.

An effective third-party cyber risk management solution helps identify, quantify and remediate security risks to prioritize threats found within an organization's vendor network. Most of these solutions utilize a risk scoring system to make it easier to identify and mitigate serious vulnerabilities faster. As network environments and attack surfaces grow in complexity (across network, databases, applications, IoT devices, containers, etc.), risk scoring has become essential to prioritize limited security resources for maximum benefit.

The average total cost of a data breach was **$3.92 million** in 2019.

The Need for Accuracy

The need to accurately represent risk via scoring is essential. To do so, it's important to determine cyber risks based on an organization's security posture in light of its environment and in terms of its digital assets and the threats targeted against it.

To do that effectively, multiple dimensions within an organization need to be investigated and combined into risk categories that try to characterize particular events. These risk categories are meant to highlight levels of severity and impact for the company, making it easier to communicate risk in a way that's manageable and understandable for the company under evaluation.

Multiple aspects within an **organization** need to be **investigated** to develop risk categories.

Level Playing Field

Measuring risk needs to be done consistently across all organizations to be fair to each one being evaluated, regardless of size, digital footprint, or levels of revenue. This includes consistency in how the company is being evaluated and which information is going to be used. The scores are meant to draw attention to the specific areas or challenges that need to be addressed by that company, either to remediate an identified issue that needs to be resolved or in some cases, prevent additional exposure to areas that may have already been exploited.

Determining the Score

When evaluating risk, data is collected and organized into multiple categories, where weights and risk levels are assigned based on the severity posed by the results. This is done based on external observations, examining internet assets held by a company and then observing traffic to and from those assets to determine what risk is posed to them, either by the environment they're in or the posture they exhibit.

The goal is to construct something that's fair and that shows the increasing risk for large severity items. For example, a high-risk score would result from finding multiple high severity items. Finding a large amount of low severity items can also be considered high risk and should be graded the same. When analyzing data, lots of little things may equal one or more big things when taken in aggregate.

The scoring function is in place to aggregate the risk scores and illustrate multiple scenarios in a way that's trying to level out with the fairness of it, i.e. yes, there still is a problem if you have a number of low-risk items as opposed to a one or two that are high risk.

Taking an Iterative Approach

To ensure the accuracy of a score, data needs to be evaluated over a set period of time to obtain a clear and complete picture. Not all observations are apparent on any given day. Analyzing data over a period of time allows a set window to be put in place so that multiple observations can be collected and analyzed to determine how things might have changed over time. All of these observations are combined into the evaluation when developing a score. The data might show that everything is neither all bad or all good, but it's taken in the context of what exactly happened and did things change over that period of time.

When determining an accurate score, changes in data access, data gaps, company footprint and even changes in cybersecurity risk need to be factored in. Attackers don't stand still when it comes to trying to exploit computer systems or gain access to an organization's data and information. Organizations shouldn't either.

Organizations need to keep up to date with the threat landscape to gain an understanding of the latest trends in attacks and defenses and what might be affecting a particular industry.

Each change can pose different levels of impact and severity to the company. For Example:

What do new attacks look like?

How would they manifest themselves?

What measures need to be put in place to fully protect the organization?

Attackers don't stand still when it comes to trying to exploit computer systems... Organizations shouldn't either.

Risks are grouped into buckets with different levels of severity, starting from the lower risk level.

The data collected needs to accommodate change since this all takes place over a period of time and reviews how the company regards themselves against cyber threats. Change in terms of:

Threat Landscape

The Company and its Assets

The Company's Security Posture

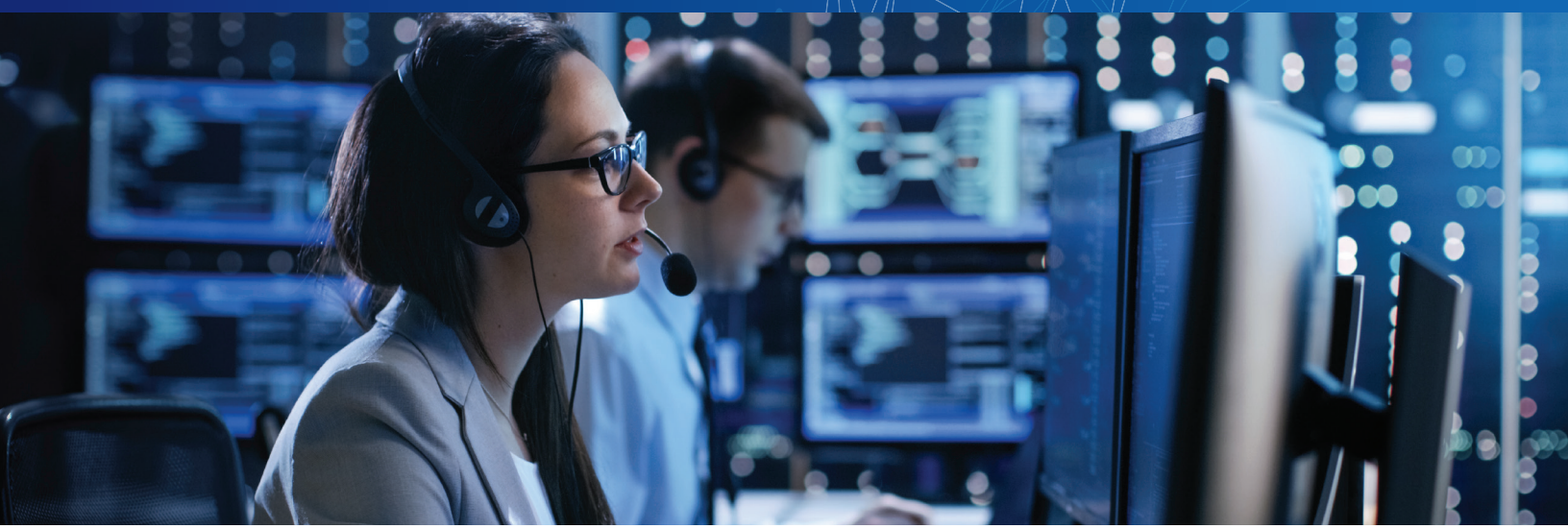
The data used in determining scores come from multiple dimensions that on any given day can be good or incomplete. By taking an iterative approach, you're able to effectively analyze data to help fill in the blanks and deliver more accurate results.

Scores are the Sum of Observations

Scores themselves are based on external observations and how those observations of potentially bad or risky activity are aggregated. Data is collected, analyzed and aggregated over a period of time to determine the level of risk. Various formulas are utilized, with risks grouped into buckets with different levels of severity, starting from the lower risk level on up.

Findings are talked about in terms of discrete observations related to a company. Those observations are done in light of a particular class of threats, which are then aggregated together in what is called a risk category. Each category represents different levels of risk within a particular space and is assigned to certain buckets so that they are weighted appropriately. A total score is then generated from all of these.

Risk category scores are rendered as a value between zero and 100 based upon the risks posed in that category. **This scoring system allows organizations to quickly identify areas of risk that might need the most attention.**



The Risk Categories

So what are the categories that are used when measuring risk? Typically, organizations are reviewed based on the following risk categories: eMail Security, IP Hygiene, Vulnerability Detection, Adversarial Threat, and Malicious Activity.

Email security, IT Hygiene, and vulnerability are much more predictive in nature and indicative of potential compromise for a company. Adversarial Threat and Malicious Activity are more of an indicator of either an active compromise or at least some sort of malicious activity emanating from that environment.

Each category is somewhat different from one another because of the different ways of managing risk within them.

The Company is in Control

Most risk categories and their scores are actually under the control of the company that's being evaluated. Companies can't do much about external adversarial activity, but they can be informed about the threat landscape and the attacks they're exposed to.

To ensure a low score, organizations need to understand what the threat landscape looks like from their perspective and evaluate their security defenses to limit exposure to risk.

The BlueVoyant Difference

Most security ratings platforms focus on publicly accessible, external data sources to assess and benchmark vendors, with each applying their own methodologies to analyze and evaluate a company's security posture. While good, this information can lead to an incomplete picture or a high rate of false positives.

BlueVoyant is able to leverage insights gained from our managed security services and threat intelligence to integrate what we see driving risks for companies and tie that back to our managed risk offerings.

The threat landscape and the risks associated with it are constantly changing. By codifying our cybersecurity expertise into our risk offerings, BlueVoyant is able to integrate the knowledge we've gained through actively investigating and remediating cyber attacks into our risk services as they occur.

Risk changes over time. Make sure you have an adaptive risk service that can keep up.

With BlueVoyant, you can be confident in the fact that our scores are:

Fair **Complete** **Consistent** **Unmatched** **Up to Date**

BlueVoyant.
Frontline Defense for Third-Party Risk.

BlueVoyant Headquarters 335 Madison Ave, Suite 5G New York, NY 10017
contact@bluevoyant.com **(646) 586-9914**