VERA

VERA SECURITY SOLUTIONS BRIEF

HOW TO QUANTIFY CYBER RISK: INSIGHTS FROM VERA'S CHIEF FINANCIAL OFFICER

Introduction

Leaders often think that an increase in spend leads to an overall decrease in risk. That's not necessarily the case. For example, organizations frequently spend millions on network security controls including SIEM, Firewalls and Data Loss Prevention (DLP) only to become victims of a breach through an application code vulnerability. Depending on the size and industry of the organization, cybersecurity can be incredibly complex. New attack methods and new technologies to deal with those attack vectors show up all the time. So, to maximize efforts at assessing security risk, resources must be allocated so that the most effective tools and strategies are being used to protect the most important information assets.

According to Gartner, by 2022, 30% of Chief Data Officers will have enlisted the help of their CFOs to formally value the organization's data assets for improved data management and benefits. And by 2022, more than 30% of businesses will use financial risk assessments of their data assets to prioritize investment choices for IT, analytics, security and privacy.

.

Costello, Katie. "Gartner Identifies the Top Seven Security and Risk Management Trends for 2019." Gartner, Gartner Research, 2019, www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma

leads Risk can range from things that can cause minor set-backs, to things that can create serious problems and often weaken a company's viability. In today's world of prolific ways to share information, one of the more persistently difficult issues that the Finance team faces is how to deal with sensitive data including financial statements, customer information, and personnel data.

In certain cases, some of this data is required by constituents outside of the protective bounds of a company's IT infrastructure, such as banks that are extending credit, vendors that are vetting you, and potential M&A candidates. While laws and policies exist that provide some protection, the truth is that you never really have certainty where the data could end up and you have no ability to control it once it is sent. The information that resides outside of the company's security perimeter is accessible with equal permissions, meaning access is not restricted once someone gains access.

How to Assess Risk

Think of data risk in three ways: the nature of the information being held, the ability to secure it (probability that it can be exposed), and the potential financial impact on an organization. Sensitive data that comes in the form of personal, business or classified information can put an organization at risk. The second aspect, the ability to secure it, is a function of how the data is stored and distributed. Financial risk is typically the cost of lost revenue or cost of litigation..

Challenges with Identifying Risk

Revenue loss risk and litigation costs risk are tangible impacts that can be measured. Having an understanding of how vulnerable your data is important in order to assess risk. If you are SOC2 compliant your risk is going to be mitigated by the controls identified within the internal bounds of your system . The difficulty arises in knowing how data is being accessed once it leaves your repositories.

Cost of a Data Breach

It's important to understand what the risks and potential costs are is an important component of business planning. How would the company react if information was disseminated to the wrong audience? What could it cost the business? It is human nature to think "it won't happen to me" or to simply assume that the party will act with integrity and delete the information that erroneously came to them.

Managing Cyber Risk

Leaders should understand where there are exposures in either tools or processes. As technology now permeates within the Finance organization, a strong partnership with IT is critical. An important practice is to understand where sensitive data is stored and how access is provided to parties that need it, most importantly outside parties. Company policies and practices often overlook, or have no direct control, with data that goes outside of the organization so this awareness is important.security gaps are critical to cover.

Cloud vs. On-Premise Cyber Risk

Leveraging a cloud provider can be a big risk if the team is inexperienced in the cloud. That lack of experience (either from a third-party provider, or internal) leads to misconfiguration, inadvertently exposing data and applications to the public. For both cloud and on-prem - secure the data itself, do not rely on configurations. Also important to identify and align with a certification that best fits with the organization's security requirements. Performing thorough assessment helps reduce adoption risk, but perform them to deeply evaluate the solution, not to simply complete a compliance exercise.

Equations to Quantify Cyber Risk

Generally speaking risk is going to be the probability of an event multiplied by the potential cost (impact). There are a few ways to think formulaically about risk, depending on your situation. I recommend getting started with something simple and straight-forward.

Probability x impact = risk

Challenges with Quantifying Risk

Risk can be challenging when the organization doesn't know what assets they have, much less how it's classified. It's impossible to protect what you can't see. It can also be difficult even if they DO know what they have, because of the overwhelming amount of how much they have to protect.

Risk Tolerance

It's first important to get an idea of the company's risk tolerance. Are you extremely risk averse? The answer may differ depending on what needs to be protected. I mention risk tolerance, because many security leaders have focused on being technical experts, which is extremely valuable, however, it's also important to have a thorough understanding of the business' risk tolerance, or "appetite". In other words, what level of risk are you willing to accept and still be able to justify and defend to stakeholders? This gets us beyond a culture of fear, into one that empowers employees to make strategic decisions.