www.pexels.com

4 Best Practices For Third-Party Cybersecurity Risk Management

Published on February 23, 2018

Kimberly Carlos | Follow
Director of Cybersecurity Prod...

In today's fast-paced, digital world, it's not enough for your company to take a reactionary approach toward cybersecurity risk management. By doing so, you face the very real possibility of a data breach or security incident, leading to a declining consumer confidence, severe reputational damage and heavy fines. As an example in the United States, Equifax's inadequate cybersecurity standards endangered millions of Americans' private data, and the Equifax brand (and bottom line) has suffered immensely. Equifax lost more than a quarter of its stock value within a week of the breach going public, and by two weeks, its brand-reputation score from YouGov had dropped 33 percent.

To safely navigate the modern business climate, your corporation must develop and maintain an aggressive, well-defined strategy for risk management. This strategy must be woven into your organization's entire business model, including:

- Careful management of third-party vendor risk
- Objective and thorough documentation of policies and risk controls
- Ongoing education and training that reflects current cybersecurity trends
- Development of a risk-aware culture across all levels of the company

> *While most companies have some awareness about the importance of internal cybersecurity risk management, they often fail to extend that same due diligence to third-party security. Do you know your vendors' preparedness when it comes to common cybersecurity risks, like system outages, human error or data breaches? Unless your organization can demonstrate that it has taken the appropriate steps to account for and control these risks, you may be on the hook for a vendor's error.*

One important tool that will help your company identify and improve gaps in third-party vendor risk – and other areas of exposure – is a Vendor Risk Assessment. In general, this assessment identifies the elements and systems that form your current risk outlook, quantifies your levels of inherent and residual risk and hones in on areas for improvement. With this tool, you will better understand the probability and severity of potential cybersecurity incidents. You will also gain a firmer grasp on the controls you have in place – or should have in place – to mitigate the likelihood and impact of an incident. When carrying out your own assessment and evaluating your third-party cybersecurity risk, here are some important standards to consider:

It Starts With You: Setting Up a Successful Vendor Risk Scoring System

As any relationship guru will tell you, it's best to work on yourself before you work on someone else's flaws. This philosophy is just as critical to mitigating third-party risk. Before assessing your third-party vendors, you should understand your internal inherent risk – the potential flaws in your own system before controls are implemented – and clearly define your organization's risk tolerance. After identifying the inherent risk in each outsourced activity and defining risk ratings by activity type (i.e, financial, legal, marketing, IT, sales, operations), your team can use these parameters to create an objective vendor-scoring system that measures against your risk appetite. Armed with these documented guidelines, your team can determine the required depth and frequency of security controls for each vendor. When building these controls, it's important to consider three key features of a vendor:

- Accessibility to your data
- Accessibility to your systems
- General accessibility (such as the vendor's potential impact on finances or brand integrity)

By creating a risk questionnaire centered around these vendor features and assigning a point-based value system that measures against the risk appetite previously defined by your organization, measurement becomes standardized, and it offers a more realistic look at your complete vendor-risk landscape. As a result, your organization can appropriately allocate risk management resources, efficiently determine the necessary cadence of risk management activities and improve overall risk management outcomes.

Understanding Your Vendor Risk Outlook Leads to Practical Applications of Scoring

After you begin to rate your own vendor risk, one thing will become clear: not all vendors are created equal. To optimize risk management, it's important that each is treated on an individual basis (within the larger systemic approach described above). Your vendor for office supplies doesn't need the same level of scrutiny as your payment processor, for example.

Talking with people in your organization who work directly with third-party providers, like account managers, should give insight into the criteria and requirements needed to assess each vendor's risk. For example, a vendor that utilizes cloud-based technologies requires a more critical evaluation to reflect the increased risk posed by those technologies. The most risk-prone vendors can be easily identified using your scoring system, providing insight about where to allocate resources and how to grant access to your data. In this way, the categorization of riskier vendors can highlight security and due diligence gaps, help control risk management costs and facilitate effective demonstrations of your successful risk management program to senior leadership.

Don't Let Stagnation Diminish Your Cybersecurity Risk Management Strategy

Cybersecurity administrators are given a near-impossible task: Predict and mitigate the next big threats. However, this demand becomes much more manageable after implementing a consistent cadence of education, training and regular updates to your risk management plan. It's not enough to implement a risk management program and then rest comfortably on your

laurels. This is true not only for setting time-frames of risk assessment and reflecting current cybersecurity trends – it's also a valuable philosophy for avoiding stagnant thinking when it comes to the identification of and protection against potential risks.

From the boardroom down, it's important to include a diversity of thought in your risk management strategy. Not everyone operates a computer, shares data or manages risk in the same way, and counterarguments to the prevailing wisdom should be encouraged as part of a healthy debate. Including diverse parties in this process allows your risk management team to improve outcomes in several ways:

- Your risk management team can avoid group-think and false harmony, leading to a greater chance of discovering previously unknown risks, exploits and exposure points.
- An inclusive approach to risk management will increase all participants' buy-in toward a risk-aware culture across the company.
- Your organization can refine its vendor scoring system to establish better standards for determining the most viable threats, as opposed to those that only give the perception of importance (but have a low chance of actually occurring).

Even if your company has a strong risk management plan in place, including accurate scoring of third -party risk, it's important to remain vigilant in the face of new threats. The financial and reputational costs of failing to reasonably safeguard against risk are exponentially higher than the costs of regular upkeep and maintenance. If you and your vendors don't have affirmative answers to the following questions, then there may be reason for concern:

- Do we have a clearly-defined process for onboarding and scoring new vendors?
- Do we have a consistent schedule for updating and maintaining vendor risk scores?
- Are we taking appropriate steps to stay up-to-date on federal and international regulations, emerging threats and industry-wide best practices?
- Do we provide regular education and training opportunities to our employees?
- Do we execute consistent penetration testing to ensure our risk controls remain adequate as our business changes and expands?
- Are we tracking and limiting third-party exposure through risk management tools and software?

By implementing these proactive controls, your company will be in the best possible position to "future-proof" your risk.

Avoid Knee-Jerk Reactions By Leveraging A Comprehensive Tool For Vendor Risk Management

Following the steps listed above will leave your company well-positioned to manage third-party risk and limit exposure to cybersecurity incidents. And perhaps most importantly, this system can impart objectivity in the event of an incident. It can be easy to make snap judgments based on immediate events or negative headlines, but developing a proactive plan forces your organization to answer tough philosophical questions before a crisis. For instance, do you know how your company (or a critical vendor) would react to a ransomware attack? Some organizations may choose to accept the potential disruption to service or loss of data while their IT team develops a solution. Others may choose to budget for and pay the ransom to preserve equilibrium. Either way, the important part is to prepare for that contingency and related issues in an objective manner.

To reach these high-level decisions, it's essential to have all elements of your risk management strategy, including a register of third-party vendors and their risk scores, accounted for in one location. A IT Vendor Risk Management platform is a great place to start. Check out our website to learn more about our IT GRC solutions.

Kimberly Carlos
Director of Cybersecurity Prod...

Follow

0 comments

Sign in to leave your comment

More from Kimberly Carlos 8 articles

NYDFS Cybersecurity Requirements for...
December 4, 2017

Webinar: How to Simplify Your IT Vendor Risk...
November 14, 2017

Webinar Replay: Prevent a Ransomware...
August 30, 2016