IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Catching the Blind Spots of Vendor Risk Management

Tom Turner

Tom Turner
CEO and President
BitSight

Biography

Tom Turner is CEO and President of BitSight (https://www.bitsighttech.com). Tom has extensive security industry experience, and has helped build category-defining companies. Prior to joining BitSight, Tom was a founding member of the executive management team of IBM Security Systems, a new division within IBM Software group that was created on the heels of the Q1 Labs acquisition.

Formerly, he was Senior Vice President of Marketing and Channels at Q1 Labs, where he was responsible for all product management efforts, demand-generation programs, and channel sales and marketing initiatives. Before joining Q1 Labs, Tom served as Director of Marketing for endpoint security at Cisco Systems, where he helped elevate the company to the number two position in the host-based, IDS/IDP market.

Keywords Cybersecurity, Security, Risk management, Cyber risk, Vendor risk management, Third-party risk management, Cyber insurance
Paper type Opinion

Abstract

In this article, the author looks at a number of common blind spots associated with vendor risk management (VRM), or 'third party risk management'. The article shares the six top misconceptions surrounding VRM and suggests strategies for businesses to overcome or avoid some of these pitfalls.

Introduction

In my experience there are a number of common blind spots associated with vendor risk management (VRM), or 'third party risk management' as it is sometimes called. Managing hundreds to thousands of vendors, suppliers, outsourcers and other third -party relationships is difficult in the best of times, and as companies increasingly rely on third party vendors to meet their operational needs overcoming misconceptions surrounding VRM is paramount.

1. Only the highest value business relationships have the most inherent risk

Today we see many high profile data breaches hitting the headlines. Businesses are now more connected than ever before, and organizations are having to deal with increasing numbers of third parties. Often, there will be a direct relationship where data is exchanged. However, we are seeing more indirect relationships where a third party may not be deemed critical to the organization's service or product, yet they still have the potential to introduce

risk. Take the Netflix 'Orange Is The New Black' leak in April last year from Larson Studios. This was a post-production company that was probably thought to be a distant vendor in the supply chain, yet when they were hacked it had a massive impact on the core business.

Likewise, many businesses are using the same third party, which is often unavoidable. For some products and services, there is only one dominant player in the market to choose from if you need to outsource. This situation can result in massive downstream effects if there's a data breach, compromise, or service disruption. For example, the NotPetya malware hit many companies in Ukraine particularly hard, such as the shipping giant Maersk. This happened because a Ukrainian based software accounting platform was compromised, and the ransomware spread to its customer base.

Breaches and outages aren't just resulting from typical third parties anymore. They're also stemming from more distant vendors. While these organizations may not have access to your network, you may rely on their technology or services which could cause considerable risk downstream.

2. Your most trusted form of assurance is a diligence questionnaire

VRM programmes have traditionally focused on setting contractual obligations for vendors. Risk managers would periodically check on whether vendors were meeting certain obligations and move on to the next item on their "to do" list. For a long time, the only way to manage risk was to use questionnaires, audits, and penetration tests. This has changed, and businesses are now actively 'hunting' for risk. They are consuming multiple data feeds about operational, financial, and cyber security risk. In doing so, many organizations have taken a more collaborative approach with vendors, rather than a combative one. The notion that VRM is a game of strong arming between risk and legal departments is changing. Organizations and their vendors are having more constructive dialogues.

3. VRM is not a Board level issue

According to Gartner, 80% of security risk management leaders are being asked to present to senior executives on the state of their security and risk programme and 75% of Fortune 500 companies are now expected to treat VRM as a board level initiative to mitigate brand and reputation risk. Boards are beginning to request updates more than once a year and this has led to the emergence of security committees.

The challenge for risk managers is how best to contextualize the company's level of risk. This is where objective, quantitative measurement can really help. For example, being able to say that the aggregate level of cyber risk posed by vendors has dropped 20 percentage points is a lot more insightful than saying, "We've mandated that all of our vendors implement multifactor authentication." It's important to learn how to speak the right language to the Board[1].

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

4. Regulations and VRM programmes are two different issues

The impact of regulation very much depends on the industry sector, but if you are subject to any regulation at all, then it needs to be included in your VRM programme. Regulations that encompass all industries, such as General Data Protection Regulation (GDPR) which came into force on 25 May this year, needs to be part of the risk management programme of every single organization. Article 32 states that organizations that collect personal data must have rigorous due diligence processes to ensure that appropriate controls are in place before sharing data with vendors.

5. VRM can be handled manually with existing resources

Relying solely on subjective point-in-time questionnaires can leave a lot of risk unidentified or unaddressed. Many companies now understand that having a continuous objective view is needed. Also, you can't simply just throw people at this problem. There are too many vendors connected to the enterprise and not enough risk professionals in the world to manage them. Companies need to automate processes whenever possible to manage this risk. There is going to be a huge breakthrough when businesses across all sectors recognize the importance of automation and allow human intervention when urgent action is required.

6. Engaging with vendors and the supply chain to correct risk is difficult and confrontational

Companies have different approaches for engaging with vendors and some have more influence than others. However, we are learning that presenting data and accessing a common platform provides significant benefits.

Giving non-customers free access to a security ratings platform via a trusted partner will allow third party vendors to investigate potential network issues and allow access to remedial resources. This is a good example of how engagement with vendors can be driven by objective data. It also offers vendors a benefit in return for their engagement and reduces some of the confrontation that can accompany risk assessment.

In conclusion

Outsourcing is nothing new. Industries have been embracing service providers for functions they either couldn't or didn't want to perform for years. With economies of scale at play, there are potentially long-term benefits. With many organizations using the same vendors to rectify issues, we can reach a wider audience and the whole digital economy is better off.

Reference	
1	https://info.bitsighttech.com/5-ways-cios-optimize-communication-guide