SAI360

Strategically Manage Vendor Risk and Build a Stronger Cybersecurity Posture

SAI GLOBAL

VENDOR RISK MANAGEMENT PROVIDES VALUE EVEN BEFORE RISK EVENTS OCCUR. IT REDUCES THEIR LIKELIHOOD AND SEVERITY, AND IT WILL REASSURE CUSTOMERS AND PARTNERS WHO WANT TO SEE YOUR RISK PROFILE BEFORE INVESTING OR TRANSACTING.

Cleverly manage those that manage your sensitive data

For most modern businesses, Vendor Risk Management (VRM) is increasingly important as the number of cyberattacks and data breaches suffered by organizations large and small continues to grow. These risks will no doubt continue and almost certainly intensify in their frequency, sophistication and severity.

Yet for all their significance, many companies remain vulnerable to these attacks. In its October 2017 Global State of Information Security Survey (GSISS), PwC notes that while breaches have become more common, "many organizations worldwide still struggle to comprehend and manage emerging cyber risks in an increasingly complex digital society. As our reliance on data and interconnectivity swells, developing resilience to withstand cyber shocks … has never been more important."[1]

Vendor Risk Management focuses its attention on managing the risks emerging from third- and even fourth-party vendors. Unlike SRM, which focuses on physical supply chains, VRM focuses on "logical" or "information" supply chains.

Critically, Vendor Risk Management is an important tool for protecting data. As the global economy and the companies, governments and other organizations it comprises become increasingly digitized, we are gathering more data on customers and employees alike – shopping histories, browsing and reading habits, health and legal information, and more. This data is a rich source of value, so managing the risks around it is vital.

Why does Vendor Risk Management matter?

Businesses that can't protect their data face the prospect of losing the value they can generate from it. Worse, they face potential financial, reputational and legal harms if they are breached and the data stolen, not to mention the harms done to the subjects of the data breach.

And businesses are not prepared. PwC further notes that 44% of respondents to its GSISS survey don't have an information security strategy in place, and 39% expect "loss or compromise of sensitive data" to be a consequence of a successful cyberattack.[2] Third-party vendors like AWS, Google, and Microsoft offer cloud-based services that play a key role for many modern organizations. They provide backup, storage, computing, analytics, business process automation, information publishing and more using consumption-based, "as-a-service" (aaS) delivery models. They also integrate with "on-premises" systems to create hybrid services in cases where important data, highly sensitive data or processes must be stored or handled locally.

BEING COMPLIANT IS NOT THE SAME AS BEING SECURE.

It's a model that's only going to grow. Research by IDC found that "the global public cloud services market grew by 28.6% year over year in the first half of 2017 … Organizations not on the public cloud will be increasingly isolated."[3] This is a slow burn – businesses have been sharing and processing data for some time and it's now occurring on a vast scale, which makes managing these relationships, and the risks attached to them, more important than ever.

As always, the starting point is to cleverly integrate effective risk management practices into your internal systems and processes. These practices should then be extended to the third parties that you deal with. Such measures come to the fore in highly regulated industries, but even in less-regulated (or non-regulated) verticals, businesses must guard themselves against exposure to vendor-based risk.

A DATA BUSINESS IS A RISKY BUSINESS

Customer data safety is a critical risk factor and **if you suffer a risk incident**, customers won't discriminate between your company and its vendors – **they'll blame you**. That means your reputation and finances, not those of your vendors, will bear the brunt of the damage.

This includes immediate harms – including possible loss of existing customers, contracts and partners, legal or regulatory penalties, increased insurance costs and a hit to your reputation – as well as the opportunity cost of future harm, as customers may be reluctant to trust you with their business (funds, data, relationships).

For example, credit services company Equifax's data breach, which has affected as many as 143 million customers, "may cost the company hundreds of millions of dollars and hurt its reputation for years to come," according to CNBC.[4] Similarly, the fallout – in terms of reputational and financial losses – attending other high-profile data breaches, such as those suffered by Home Depot (more than $179 million[5]), Sony ($99 million in losses and a 10% drop in share price[6]) and Target (nearly $300 million[7]), has been well-documented.

If your business shares information with third parties, it's vital that your risk management encompasses their activities too. Verizon notes in its Data Breach Digest that to manage and control risk, "you must first assess it accurately," and also highlights the importance of holding "complete knowledge of all information assets".[8]

This includes knowledge of where, how and how securely they're holding your data. Only a vendor risk management program can provide you with the proper oversight into your extended vendor network's risks.

If a risk event does occur, Vendor Risk Management plays a critical role. In such events, the crisis communication playbook is clear: transparency and immediacy are paramount; customers, insurers, investors, regulators and legal bodies alike all want to know what happened and how it's being remediated. Effective VRM processes will help you gather the information you need to identify the problem and implement a solution. And harms may be reduced if you can demonstrate due diligence in risk management, for example by records like audit trails and certifications, process maps and vendor compliance reports.

But VRM provides value even before risk events occur. In part, this is due to the role it plays in reducing their likelihood and severity. Customers and potential partners are themselves becoming more risk-aware, and may want to know about your organization's risk profile before investing or transacting.

What does effective Vendor Risk Management look like?

Many data breaches are due to companies thinking that being compliant is the same as being secure. While it's true that the two are closely linked, taking a by-the-numbers approach to compliance won't deliver the best results. We recommend starting with security and risk assessments, as many security frameworks and compliance frameworks have similar requirements and controls. This should place your organization well on the path to compliance.

It should also mean that if further measures are needed to ensure full compliance with the standards relevant to your industry, then you should have a strong base on which to create them.

For any organization that collaborates and shares data with third parties, third-party vendor risk management is an essential part of an effective security and compliance regime. The key challenges it must meet include:

- Maintaining control over customer and employee data
- Building confidence that third parties are treating data securely (including verification)
- Ensuring your customers trust you with their data
- Ensuring you're not lagging behind your competitors on customer data security
- Managing vendors and keeping the right mix (out with the old, in with the new)

WITH RISK COMES OPPORTUNITY

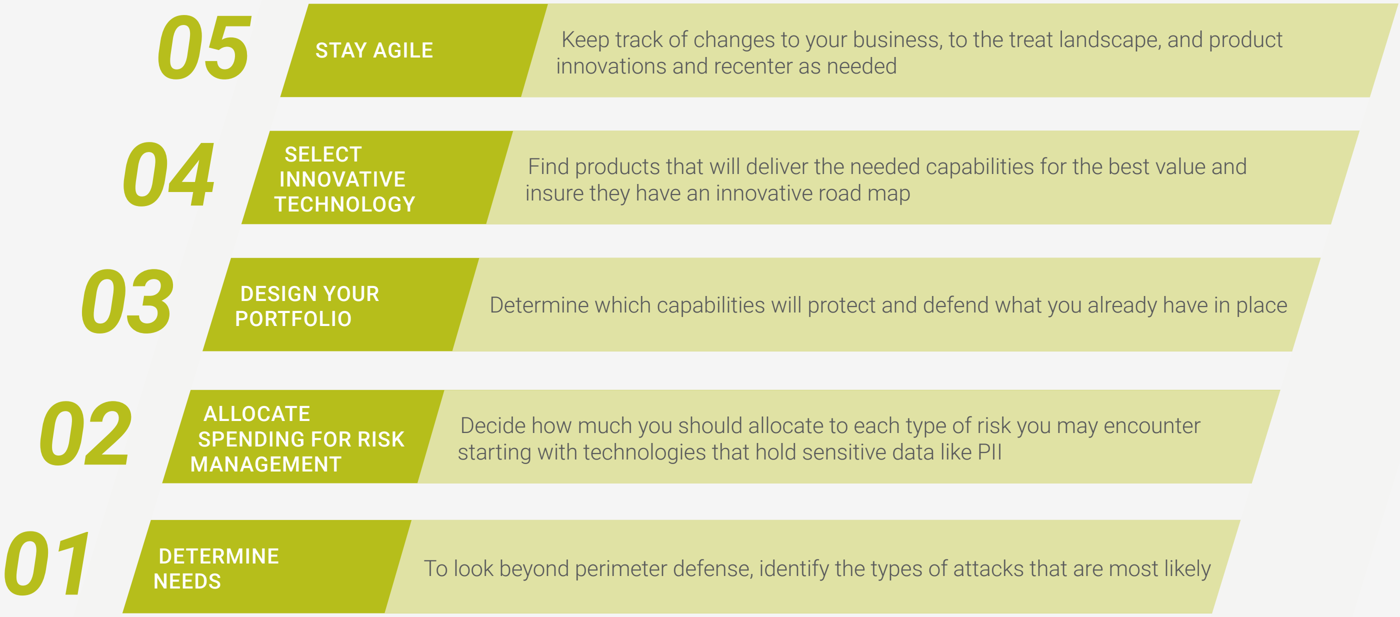
As with virtually any aspect of risk management, there is opportunity as well as hazard. Thinking of risk management as simply a matter of process and compliance loses sight of the ways in which effective risk management can generate competitive advantage. In particular, third-party risk management can help your business take full advantage of the benefits, while minimizing the downsides, of an outsourced or aaS IT business model. These advantages include:

- Reduced risk by creating a preferred vendor list
- Improved time to communicate with customers to demonstrate that you deserve their trust
- Enhanced competitiveness: With vendors – by establishing minimum performance requirements
- With buyers – by displaying proof of your improved security posture (certifications, etc.)

Organizations that take a proactive approach to third-party vendor risk management should find that these advantages translate into a more stable and profitable market presence. They should also, over time, experience the benefits of improved customer trust and even customer advocacy. This is the foundation for any successful business and is crucial to its ongoing success.

A Five Step Process for Creating a Balanced Portfolio of Security Products

Adapted from Forbes, “How CISOs Can Create A Balanced Portfolio Of Cybersecurity Products”, March 2017



05 STAY AGILE — Keep track of changes to your business, to the treat landscape, and product innovations and recenter as needed

04 SELECT INNOVATIVE TECHNOLOGY — Find products that will deliver the needed capabilities for the best value and insure they have an innovative road map

03 DESIGN YOUR PORTFOLIO — Determine which capabilities will protect and defend what you already have in place

02 ALLOCATE SPENDING FOR RISK MANAGEMENT — Decide how much you should allocate to each type of risk you may encounter starting with technologies that hold sensitive data like PII

01 DETERMINE NEEDS — To look beyond perimeter defense, identify the types of attacks that are most likely

Picking the right Vendor Risk Management solution

How best, then, to implement strong a VRM automation technology tool? First, it's important to implement a modern digital risk management platform. **Old-school techniques, like using customized spreadsheets, don't offer the flexibility that's needed**, and they can't automate important processes like data gathering and analysis.

There are numerous software platforms available, each with specific strengths and capabilities. Gartner[9] suggests that, absent of other company-specific requirements, a good solution should include these capabilities and tools:

- Risk assessment process and workflows
- Collaboration
- Contract management
- Control assessment and monitoring
- Exception management
- History
- Access and user controls
- Remediation management
- Third-party content delivery
- Vendor performance management
- Vendor profile management

Such a suite of risk, relationship and performance management tools, in combination with the ability to provide meaningful analytics and produce insightful, easy-to-understand reports and business intelligence, should enable you to **manage your vendors and ensure they're managing your data – customer, financial, transactional and other – as carefully and securely as you are.**

FINDING THE RIGHT SUPPLIER

Many different vendor risk management solutions are available, featuring a range of capabilities, add-ons and industry-specific functions. But a good supplier will offer more than just a technology platform. You should look for an organization that's willing to become a trusted ally.

A good supplier will help your organization plan its vendor risk management implementation. This includes: assessing your current situation; identifying any gaps or weaknesses a malicious actor could exploit; providing tools for evaluating your third-party suppliers; and so on. It will also help with the rollout, not just in terms of the technology platform but also with messaging and training, and of course supply ongoing support, upgrades and advice.

CUSTOMERS WON'T DISCRIMINATE BETWEEN YOU AND YOUR VENDORS IF YOU SUFFER A RISK INCIDENT. THEY'LL BLAME YOU, AND IT'LL BE YOUR REPUTATION AND FINANCES THAT TAKE THE HIT.

Conclusion

Many organizations simply don't know how well they can trust third-party vendors with their own customers' personal data unless they have a VRM program in place. An effective third-party vendor management implementation will help you ally with reputable third parties, verify their capabilities and move your business forward with a single, unified, accurate understanding of your risk posture "truth."

[1] PwC, 2017, Strengthening digital society against cyber shocks: Key findings from The Global State of Information Security Survey 2018.

[2] PwC, CIO and CSO, 2017, The Global State of Information Security Survey 2018.

[3] IDC, 2017, Worldwide Semiannual Public Cloud Services Tracker.

[4] CNBC, 8 September 2017, 'Equifax shares plunge the most in 18 years as Street says breach will cost company hundreds of millions'.

[5] Web Titan, 14 March 2017, ' Cost of a Retail Data Breach: $179 million for Home Depot'.

[6] Egnyte, 12 June 2017, 'How Much Does a Data Breach Cost a Business?'.

[7] The SSL Store, Hashed Out, 26 May 2017, 'Cost of 2013 Target Data Breach Nears $300 Million'.

[8] Verizon Enterprise, September 2017, "Data Breach Digest Update: Data ransomware – the Catch 22

[9] Gartner, 2017, Magic Quadrant for IT Vendor Risk Management. Note that Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

REFERENCES

Vendor management generally
    http://www.zdnet.com/article/why-it-vendor-management-makes-sense/
    https://www.cio.com/article/2437750/outsourcing/why-you-should-create-a-vendor-management-office.html
    http://www.rmmagazine.com/2017/08/01/improving-vendor-risk-management/

Gartner definition
    https://www.gartner.com/it-glossary/vendor-risk-management/

Gartner magic quadrant
    [Supplied]

Data breaches
    https://securityscorecard.com/blog/third-party-security-vendor-risk-problem/
    https://www.ibm.com/security/infographics/data-breach/
    http://www.pwc.com/us/en/cybersecurity/information-security-survey.html
        Equifax
        Target
        Sony: https://www.egnyte.com/blog/2017/06/how-much-does-a-data-breach-cost-a-business/
        Home Depot: https://www.webtitan.com/blog/cost-retail-data-breach-179-million-home-depot/

[solutions] to advance confidently

About SAI Global

SAI Global helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability. Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk. To see our tools in action, request a free demo.

We have global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific.

For more information visit www.saiglobal.com/SAI360.

SAI GLOBAL