Scrut Automation

Effective
Vendor Risk Management

Contents

Introduction

Vendor risk management (VRM) has become an integral part of GRC in today's threatening cybersecurity environment. As businesses and their vendors grow more digitally connected, a vendor's security problem can, by relation, become a source of risk for its customer. For example, if your vendor has custodianship of your data, then deficient vendor data security practices can expose your data to risk.

However, as enterprises grow more connected and interdependent through technologies like application programming interfaces (APIs) and cloud computing, the potential spillover from a vendor's cyber vulnerabilities becomes far more serious. Some recent massive data breaches reveal how weakness in vendors' defenses opened up attack paths into major corporations.

To solve this problem, it is necessary to adopt a more integrated and comprehensive approach to vendor risk management. GRC managers need a unified view of vendors' security postures and risk profiles. New automated solutions, such as Scrut, can help. They offer enable faster, smoother, smarter vendor risk assessment, monitoring, and management.

Scrut Automation

Understanding The Need For Vendor Risk Management

Vendors expose your business to a wide variety of risks by broadening the attack surface. A defective part in a manufactured product, for example, can result in legal liability and regulatory scrutiny. Vendors can drive various financial and operational risks, as well. For instance, if a creditor seizes the part maker's inventory in a bankruptcy proceeding, that could cause your supply chain to fall apart—leading to late deliveries, unhappy customers, potential losses, and litigation.

These risks keep lawyers busy, and indeed most vendor agreements contain all sorts of indemnification and "hold harmless" language. Ultimately, though, the onus of managing vendor risk is with your organization. You can blame the vendor, but your reputation is the one that will suffer. You have to stay on top of vendor risk profiles and track potential dangers before they cause damage. Nowhere is this more serious than in the realms of cybersecurity and compliance.

Like all businesses today, your vendors are vulnerable to attack by increasingly sophisticated malicious actors. Their systems and data can be frozen by ransomware attacks. If your vendor has your proprietary intellectual property on its systems, it can be breached. This is a situation that affects military contractors, for example, who may entrust top secret digital designs to vendors with poor security postures. A number of shocking breaches in recent years reveal this risk to national security.

Less dramatic but no less impactful, vendors may store personal identifiable information (PII) about your customers on their systems. If the vendor gets breached, you may find yourself dealing with privacy laws like Europe's GDPR or California's CCPA. An expensive incident response, fines, and remediation are sure to follow, even if your vendor is at fault.

Other risks from vendor risk include:

Legal or compliance problems, which can be particularly acute for companies that work government or financial services, or as military contractors.

Violations of the Health Insurance Portability and Accountability Act (HIPAA), which mandates the protection of protected health information (PHI). HIPAA violations can lead to costly fines and reputation damage.

Legal liability, inclusive of lawsuits, class actions, and termination of contractual business relationships.

How Vendor Risk Management Has Changed In The Age Of The Cloud, APIs, And Interconnectedness

We are in a new era of vendor risk. Between cloud computing, APIs, and increased interconnectedness between business partners, businesses have been exposed to new, broad attack surfaces. Poor cyber defense on the part of a vendor can now lead directly to a breach in your infrastructure. A number of high-profile hacks bear out this risk—with hackers compromising a vendor's network and exploiting it to find a path into a much larger and more valuable target.

Even simple oversights can cause serious difficulties. For instance, enforcing security policies can be challenging in the cloud. A well-meaning but ill-informed developer could easily put sensitive data on an unprotected cloud volume and not tell anyone. This sort of thing frequently happens, with serious consequences for his or her employers and their customers.

The Benefits Of Vendor Risk Management

A well thought-out and implemented VRM program will deliver a host of benefits. For one thing, it will reduce your third-party security risks. VRM makes it less time-consuming and resource-intensive to deal with future vendor risks. Accountability for your company and your vendors will be better understood by both parties. VRM helps ensure that your service quality or availability will not suffer. You can cut costs in vendor management, and improve your overall financial efficiency. VRM lets you focus on your core business and less on grappling with vendor-borne risks.

Reduces Third-Party Security Risks

Saves Time And Resources

Better Understanding Of Accountability

Protects Service Quality And Availability

Reducing Vendor Risk Through New Strategies And Technologies

A new generation of GRC tools makes it possible to become more effective and consistent in vendor risk management workflows. They enable you to pursue new vendor risk management strategies, such as conducting more frequent audits and engaging in continuous risk monitoring. They also give you the ability to stay on top of vendor risk profiles with automation and a unified vendor risk management interface.

New Vendor Risk Management Strategies

Today's more threatening cyber environment demands more thorough and meaningful vendor risk management strategies. It might have once been sufficient to have vendors fill out a form asking basic security questions when they were onboarded and perhaps annually after that. That is not longer enough.

VRM requires a strategy. The good news is that you have a variety of VRM strategies to choose from. At a high level, effective VRM means doing deeper security reviews and audits. It is necessary to probe vendors' security capabilities and controls. And this needs to happen more frequently. VRM strategy might involve doing more to define your vendor selection process, developing new, better governance documents and processes, establishing contractual standards, and formalizing the vendor due diligence process. Robust reporting must always be part of any VRM strategy.

VRM strategy might include:

- Defining a vendor selection process
- Developing better governance documents and processes
- Establishing contractual standards
- Formalizing vendor due diligence process
- Robust reporting

Developing An Effective Vendor Risk Management Program With New Technologies

It is challenging, if not impossible, to execute on new vendor risk management strategies without the benefit of new technologies. Spreadsheets and emails might have been up to the job in earlier times, but they will no longer suffice. Instead, a new generation of vendor risk management solutions provides the functionality required to conduct the frequent, in-depth security reviews and audits—and then monitor vendor risk profiles in real time through a single interface.

Developing an effective VRM program:

Automating Vendor Security Profiling

- Creates a vendor security profile
- Accelerates security review

Unified Storage

- Centralize vendors' security information
- Easy sharing with customers and auditors

Single System To Facilitate Secure Collaboration With Vendors

- Manage changes to vendors' security profiles
- Remediate control deficiencies surfacing from changes

Aligning VRM With Business Processes

- Enables immediate access to relevant vendor security information
- Integrates with internal teams and processes

Mapping Risk Mitigation To Vendor Risk Profiles

- Helps organize the communications and remediation steps with the vendor
- Track processes compared to specified remediation timeframes

Automating Vendor Security Profiling

Done right, the vendor risk management process will create a meaningful vendor security profile. This usually means having the vendor respond to a questionnaire about its security practices. The problem with this process was that it created manual tasks for those tasked with vendor risk management. They might have to retype answers into spreadsheets, or worse, simply store the filled-out questionnaires on a file drive. Follow ups tended to get delayed or forgotten altogether. The new breed of vendor risk management solution automates the full cycle of conducting vendor security reviews. Some, like Scrut Automation, enable you to upload your own security questionnaire. The solution then automatically emails questionnaires to vendors. Responses are automatically listed in a searchable, unified view of vendor risk profiles. The net effect is to accelerate security reviews. Users can determine, at a glance, if a vendor's security policies match your own. The solution will flag vendors that are out of compliance, with automated follow up processes to bring vendors into compliance.

Unifying The View/Place To Store Vendors' Security Postures And Risk Profiles

Staying on top of vendor risk in today's security environment means doing a better job of organizing vendor risk information. New vendor risk management solutions make this possible by establishing a single place to store all vendor certifications, proofs of compliance, software vendor audits, and other paperwork related to vendor security. Such centralized storage makes it easier to share vendors responses with customers and auditors as needed.

Creating A Single System Of Record To Facilitate Secure Collaboration With Vendors

Not only does a vendor risk management solution like Scrut centralize vendors' security information, it also provides a single system of record for all risk-related interactions with vendors. For instance, as vendors' security profiles change, it will become necessary to collaborate with them to remediate control deficiencies and the like. The vendor risk management solution gives users a single, authoritative source of information about how vendors are doing with such tasks.

Aligning Vendor Risk Management With Business Processes

Vendor management usually comprises one element of many different business processes. The marketing department, for example, may select an email campaign vendor from a procurement platform. That selection process should be aware of vendor security risk, in that it would be unwise to entrust the company's email list to a vendor with a security problem. However, this kind of mistake happens all the time. The culprit is siloed systems.

In theory, information about vendor risk should be present in a company's procurement solution, but this is not always the case, especially if vendor risk management is done manually. There may be important information about a vendor's security posture contained in a vendor security questionnaire on a file drive, but the procurement team does not see it. That's not good.

A vendor risk management solution that can integrate with other systems offers a solution. Scrut, for example, enables stakeholders from different areas of a business, working through different systems, to have immediate access to relevant vendor security information. If a vendor's risk profile changes for the worse, everyone who needs to know will be informed on a timely basis.

Mapping Risk Mitigation To Vendor Risk Profiles

Staying on top of vendor risk in today's security environment means doing a better job of organizing vendor risk information. New vendor risk management solutions make this possible by establishing a single place to store all vendor certifications, proofs of compliance, software vendor audits, and other paperwork related to vendor security. Such centralized storage makes it easier to share vendors responses with customers and auditors as needed.

VRM Due Diligence Checklist

Here are some suggested steps to take when assessing a new vendor:

- ✓ Ask for references for the vendor's clients.
- ✓ Assess whether the vendor is financially healthy. It may be necessary to request their financial statements.
- ✓ Verify that they have liability insurance. It may be a good practice to have the vendor's insurance carrier issue your company a certificate of insurance.
- ✓ Verify that they meet any relevant regulatory compliance requirements, e.g., for HIPAA
- ✓ Conduct background checks on key vendor personnel, including criminal checks.
- ✓ Establish that the vendor can meet your specified service levels, e.g., response time for maintenance requests.
- ✓ Determine that the vendor has adequate security controls in place.
- ✓ Review contracts, including an examination of terms, service level agreements (SLAs), termination requirements and so forth.

Conclusion

Vendor risk management is essential for effective, thorough GRC. Today's cyber threat environment and high level of digital connectivity between companies and their suppliers make it all the more important.

The problem has been that relying on manual processes to track vendor risk profiles is inefficient. It leads to gaps in awareness of vendor security profiles. Vendor risk inevitably rises as a result. A new generation of vendor risk management tools, such as Scrut Automation's VRM platform, offers a solution. With Scrut, you can develop a rapid, effective, and efficient VRM program. This will include methods for evaluating, monitoring, and managing your vendor risk. You will know how your vendors are doing and whether or not their security postures fit with your compliance needs.

To learn more, visit
https://www.scrut.io/products/vendor-risk