TOP 4 AREAS OF VENDOR CYBERSECURITY TO PAY ATTENTION TO

COULD YOUR VENDORS BE YOUR WEAK LINK?

In today's environment, many organizations are investing heavily in their cybersecurity programs but often forget to invest in **ensuring their vendors are doing the same**. By taking the necessary precautions and understanding your vendor's cybersecurity posture, **you can reduce the risk of your vendors and contractors becoming your weakest link**.

At Venminder, we have reviewed the cybersecurity posture of hundreds of vendors. Here are the top 4 areas we recommend you focus on.

What type of vendors should be tested?
All medium, high and critical-risk vendors; any vendors that process, store or transmit your data

Who at the organization should review the results?
Third-Party Risk Manager with the internal stakeholder and internal/external audit team

What type of qualifications should that person have?
Broad background in Information Security and Risk Management

1 SECURITY TESTING

One of the best ways to identify weaknesses is to test the security of your infrastructure. Therefore, your vendors should be performing these tests:

Common security testing you would want your vendors to be performing at least annually include:

Internal and External Vulnerability Testing:
Testing that can identify and classify the security holes (vulnerabilities) in a computer, network or communications infrastructure. This can be performed by either an internal Information Technology Security team or by an external entity hired by a company to identify weaknesses within their systems.

Penetration Testing:
A specific form of vulnerability testing that is used to find vulnerabilities that an attacker could exploit.

Social Engineering:
Another specific form of vulnerability testing that focuses on the human element of an organization. Social engineering is the practice of attempting common attack tactics such as phishing emails on an organization's employees to ascertain the organization's level of vulnerability to that type of exploit.

RED FLAGS TO LOOK OUT FOR

When reviewing a vendor's vulnerability testing, you want to look for:

- Whether or not critical and high-risk vulnerabilities were found
- Whether those vulnerabilities were addressed and corrected
- Whether the vendor has a plan in place to prevent similar vulnerabilities in the future and lessons learned

Are your vendors doing regular internal and external security testing to ensure their systems are secure?

2 SENSITIVE DATA SECURITY

What Is Sensitive Data?
Information that needs to be protected against unintended disclosure. Protection may even be required for legal or ethical reasons, for issues pertaining to personal privacy or for proprietary considerations.

Data Security Means:
Protecting data from destructive forces and from the unwanted actions of unauthorized users. Destructive forces can be data breaches, theft or intentional unauthorized release.

Your vendor should be securing your sensitive data in ways such as:

Encryption:
The process of converting information or data into a secret code to prevent unauthorized access. Any network that transmit data should be using the most current level of encryption available. Ways to understand if a vendor is properly using encryption could include:

> Ask what encryption algorithms are used for data in transit and at rest.

> You can easily check for web-traffic encryption by looking for the closed padlock in the address bar of your browser.

Data Retention and Destruction Policies:
A Data Retention Policy documents an organization's plan for the continued storage of an organization's data. A Data Destruction Policy should cover how an organization handles data at its end of life, how they dispose of it and how its treated when it leaves their control.

Data Classification and Privacy Policies:
The process of organizing data into categories for its most effective and efficient use, as well as helps define the levels of protection that is necessary to keep it secure.

RED FLAGS TO LOOK OUT FOR

- Lack of documented data classification, retention and destruction policies
- Lack of up to date encryption standards for data in transit and at rest
- Lack of network security policies and procedures

Do you know how your vendors secure your data at rest and in transit?

3 EMPLOYEE, CONTRACTOR AND VENDOR MANAGEMENT

Your vendor's ability to ensure their employees, contractors and vendors (your fourth parties) are prepared to protect data is crucial to their overall cybersecurity. Confidentiality agreements, data security training and managing what employees, contractors and vendors have access to are all ways your vendor can ensure proper Employee, Contractor and Vendor Management. This enables organizations to drive service excellence and mitigate risks often caused by employees and outside contractors and vendors.

WHAT TO REVIEW

Confidentiality agreements, security training, management of vendors and access management are just some of the ways a vendor can offer assurance that anyone with access to your data is properly trained.

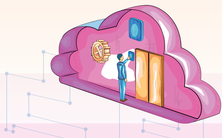
RED FLAGS TO LOOK OUT FOR

- Hiring and background checks should be done on employees
- Data and Information Security training should be performed annually with documented completion for each employee, contractor and vendor
- Access management policies should be in place and documented
- Confidentiality agreements and non-disclosure agreements should be obtained from all employees, contractors and vendors

Do your vendors perform annual information security training?

Are confidentiality agreements and non-disclosure agreements obtained from all employees, contractors and vendors?

Does your vendor perform rigorous pre-employment screening on its employees?



4 INCIDENT DETECTION AND RESPONSE

Incidents happen. The key to minimizing the impact is discovering them quickly and having a plan to address them quickly and effectively. How do your vendors handle incident detection and response?

WHAT TO REVIEW

An incident can be anything that effects the confidentiality, integrity or availability of information or an information system. This could be a data breach, a targeted phishing email attack or a denial of service attack on your vendors service offering.

Your contracts with vendors should include: obligations to notify you in the event of a breach, and if the relationship ends, notify the disposition of any confidential information.

A comprehensive Incident Management Plan (IMP) should have a detailed incident detection program that includes intrusion protection/detection tools, firewalls, anti-malware products in place to prevent/detect potential incidents as well as a patch management program.

Your vendor's IMP should include detailed steps for their incident response as well as a defined notification timeline for any breaches or incidents that impact your data. You want to be able to know with certainty that you will be notified and how quickly, should the vendor have a breach.

Incident management should include cybersecurity insurance coverage. Errors and Omissions, Cyber Crime and Sabotage are just a few coverages that offer a level of risk transfer and protection against cyber related incidents.

RED FLAGS TO LOOK OUT FOR

- Lack of notification process/timeline
- Lack of a documented Incident Response Plan
- Lack of incident detection controls in place
- Lack of cybersecurity insurance policies

Does your vendor have a documented Incident Management Plan that has procedures for detection, response and resolution of incidents?

Is a notification process clearly mapped out in your contract?

Remember, by failing to properly manage your vendor cybersecurity risk, you could become vulnerable to a breach and the regulatory, reputational and financial consequences that come with it.

Venminder can help you review the cybersecurity posture of your vendors.

LEARN MORE

PRINTABLE VERSION

Copyright © 2021 by Venminder, Inc.

venminder
Manage Vendors. Mitigate Risk. Reduce Workload.
+1 (888) 836-6463 | venminder.com