40 QUESTIONS

You Should Have In Your VENDOR SECURITY ASSESSMENT

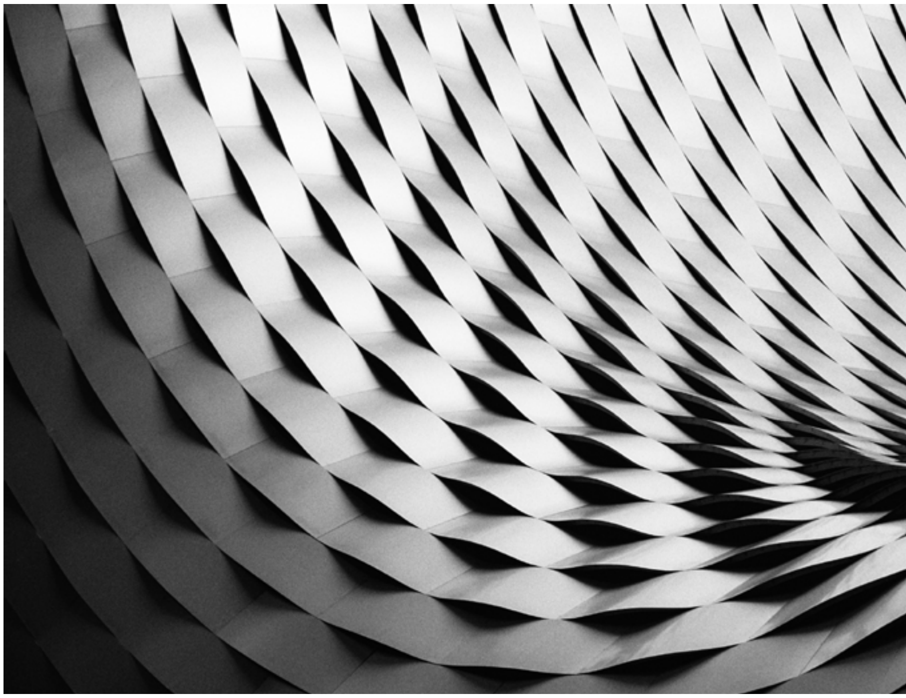
BITSIGHT®
The Standard in **SECURITY RATINGS**

You know that understanding the cybersecurity posture of your vendors is simply vital when you're getting involved in third-party business relationships.

And if you're creating a comprehensive vendor risk management (VRM) program, you know it's important to include a security assessment.

But what you may not know is which high-level questions you should consider including in your vendor security assessment. You're probably wondering what to include, which frameworks to use, and why you should be including certain questions and not others. These are all valid concerns!

Our goal with this guide is to help you get started with the creation of your vendor security risk assessment. This is not intended to be an out-of-box security assessment solution, but rather, a guide to get you headed in the right direction. We'll explain the top three frameworks you should be examining, questions you may want to consider (and why you should potentially consider them) and what else to include in your VRM program.



Getting Started

Every organization—and every vendor—is unique. Thus, many circumstances will warrant the creation of customized security questionnaires. But we suggest relying on the expertise of others for high-level questions (rather than reinventing the wheel yourself) and using industry-accepted best practices as a starting point for your assessment.

There are three industry-standard security assessment methodologies you can start with:

1. **The SANS (System Administration, Networking, and Security Institute) Top 20 Critical Security Controls—a short list of controls developed by security experts based on practices that are known to be effective in reducing cyber risks.**

2. **The NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity—combines a variety of cybersecurity standards and best practices together in one understandable document.**

3. **Shared Assessments—an organization that develops assessment questionnaires for use by its members.**

Between the three of these methodologies, there are literally **thousands** of questions that you could use. For instance, if you go to the SANS Top 20 Critical Security Controls page and select "Malware Defenses," there are 11 items beneath it that could all represent their own separate questions. Of course, we can't fit all of that information here (and we wouldn't want to even if we could!). The idea behind this guide is to give you an idea of the high-level, critical questions you should consider asking your vendors. **Let's take a look.**

BITSIGHT

Governance & Organizational Structure Questions

1

Who is responsible for cybersecurity within the organization?

This could be any number of people within the organization, but it’s important to have contact points for your vendors.

2

Is there a chief information security officer (CISO)?

You want to verify that the vendor has someone—whether it’s a director, vice president, or CISO—in a leadership position responsible for overseeing security strategy.

3

Is there a cross-organizational committee that meets regularly on cybersecurity issues?

Organizations that involve multiple perspectives are likely to have a more sophisticated approach to managing cyber risk.

4

Have you participated in a cybersecurity exercise with your senior executives?

Running tabletop drills can help an organization nail down a quick response time.

5

How do you prioritize your organization’s most critical assets?

Understanding what the organization is focused on can give you a sense of where their time and resources are going.

6 How do you specifically protect customer information?

When it comes to your data, you want to ask specifically how it is being protected—is it through encryption, access control, or other mechanisms?

7 How are cybersecurity incidents reported?

You'll likely want to see the incident escalation document showing how incidents are classified/prioritized and how everyone—from the IT security staff up through the senior executive team—becomes involved as a significant incident escalates.

8 Have you ever experienced a significant cybersecurity incident? Please define and describe it.

Defining it is one thing, but the **description** of said significant incident will be quite telling. Pay close attention to how (and how quickly) the matter was resolved.

9 When was last time you had a cybersecurity assessment performed by a third-party organization? What were the results of that?

Though assessments only provide a snapshot in time, you'll want to see that your third parties are passing their audits with flying colors—and if there are hiccups, that they're handling them correctly.

10 What were the results of your most recent vulnerability assessment or penetration test?

Look for details of the actual tests/assessments and the descriptions of the outcomes and remediation plans. Good or bad, you'll want them to be detailed.

11

Describe the experience and expertise of your IT security staff.

Experience and expertise is vital.

12

Do you outsource any IT or IT security functions to third-party service providers? If so, who are they, what do they do, and what type of access do they have?

You'll want to know this information so you can do your due diligence on any outside sources that may be able to gain access to your sensitive information.

13

What types of cybersecurity policies do you have in place in your organization today?

The policies themselves will vary—and what you **really** care about is the implementation of the policies themselves—but it's important to at least have acceptable use, remote access, and privacy and security policies in place to state the organization's expectations.

14

How frequently are your employees trained on your IT security policies, and do you use automated assessments?

Employees are much more likely to avoid downloading malware that could affect your data if they have been properly trained.

Security Controls & Technology

15 How do you inventory authorized and unauthorized devices and software?

Organizations that have an automated process for knowing what's running on their systems will have greater visibility into security incidents.

16 Have you developed secure configurations for hardware and software?

The key word here is **secure**; make sure your IT security department is involved in checking these configurations.

17 How do you continuously assess and remediate your organization's cyber vulnerabilities?

You want to know that your vendor is making cybersecurity a constant priority and is in tune with the problems that need to be fixed.

18 How do you assess the security of the software that you develop and acquire?

Having a mature application security program is a way of reducing the threat landscape inside an organization.

19

What processes do you use to monitor the security of your wireless networks?

Seek to understand how they are protecting their network against opportunistic hackers and unauthorized use.

20

Do you have a data recovery capability?

This may be the difference between **your** data being recovered or not.

21

How do you securely configure your network infrastructure?

Again, you'll want to involve your IT team to ensure that this long-form response meets their recommendations and requirements.

22

Do you have automated tools that continuously monitor to ensure malicious software is not deployed?

Most attackers are moving their efforts to the endpoint, as this is where your data is located.

23

Describe the processes and tools you use to reduce and control administrative privileges.

Not everyone needs administrative access; reducing privileges is an essential element toward creating a more secure ecosystem.

24

Do you blacklist or whitelist communications?

This process shows the vendor is taking initiative toward categorizing good and bad internet communications.

25 How do you analyze security logging information?

Check specifically how these processes are automated or if they are even being completed at all.

26 How do you monitor privileged accounts?

Escalating privileges is a common technique for external attackers, but insider threats can also loom large for your data. Make sure someone is looking at the most sensitive accounts.

27 What processes do you have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data like ours?

When configuring a data loss prevention tool, make sure it is programmed to prevent your sensitive data from leaving the environment! Many only configure DLPs to prevent certain classes of data (e.g. personally identifiable information) from leaving.

28 How do you plan for and train for a cybersecurity incident? What processes do you have in place to respond to an incident? Do you regularly practice those things?

This multipart question should provide you with better insight into what may happen in your vendor's organization should there be any security issues or concerns.

29 Do you conduct regular external and internal tests to identify vulnerabilities and attack vectors, including penetration testing, red team exercises, or vulnerability scanning?

Having a sophisticated team try to gain access is a way of improving an organization's defenses.

30

Do you have a disaster recovery plan? Describe it.

You'll want to know whether your vendor has the proper protocols in place to protect your data or assets in case of an unforeseeable emergency.

31

From whom do you receive cyberthreat and cyber vulnerability information and how do you ingest that information?

Though threat intelligence can be an important defensive tool, many organizations are not sophisticated enough to do it or do it well.

32

What types of physical protection do you have in place to prevent unauthorized access to data or infrastructure assets?

With so much emphasis on cyberthreats, it's easy to forget that sometimes physical access can be the entry point for a threat actor.

33

How do you manage remote access to your corporate network?

Remote access has become one of the most exploited IT vulnerabilities, so you'll want to evaluate how your third parties control and secure access.

34

How do you employ network segregation?

Is sensitive data walled off from other networks? Particularly sensitive customer data?

35

Do you have a removable media policy and controls to implement the policy?

Everyone knows how easy it is to walk out of most organizations with a USB full of data; does your vendor allow its employees to do this?

36

Have you identified any third parties who have access to your network or data? How do you oversee their security initiatives?

Essentially you’re asking your vendor if they have a VRM program in place, which is important.

37

How do you monitor your network to alert to cybersecurity events?

Asking your vendors to clearly describe their network monitoring—including technology—is a great way to understand their overall initiatives.

38

How do you monitor your third-party service providers?

Having a plan in place for vendor risk management is critical, but how can you be sure that third parties are meeting those efforts?

39

How do you monitor for unauthorized personnel, connections, devices, and software?

Monitoring for internal, as well as external, threats is key in securing the infrastructure against attacks.

40

Describe the process you have in place to communicate to us security incidents affecting our data.

Again, you want to clearly understand when and how your vendor will communicate to you a security incident affecting their network and your data.

Is A Security Assessment Enough?

If you work with or are on a security team, you know how difficult and time-consuming it is to create a program that will protect your organization. Most enterprises spend a number of years training staff, purchasing security technologies, and finding innovative ways to keep the company's "crown jewels" and highly sensitive data safe from those who should not have access to it.

> The more strategic information you can gather about your vendor's security controls, technologies, and governance, the better.

If you're told to take this information and knowledge and boil it down into a series of questions to pass along to your third parties, is that all that you need to ensure that your vendors are adequately taking care of your technology? **Probably not.** Unless you've been working with a vendor regularly or intimately or have helped them build their own security program, the questions you ask are likely not going to turn up as many details about their security as you'd like.

Should you still create and disseminate a security assessment? **Yes, absolutely.** The more strategic information you can gather about your vendor's security controls, technologies, and governance, the better. **But the fact is, security assessments alone do not provide the level of visibility you need into your vendor to understand how secure your data is on a day-to-day basis.**

The Missing Piece

Aside from risk assessments and questionnaires, there are plenty of steps your organization can take to build out a strong and comprehensive vendor risk management program. This includes on-site interviews, technical scans and penetration tests, and a review of the vendor's security documentation. All of these steps are incredibly important—**but they only offer a snapshot in time of your vendor's health.**

Sadly, there are organizations being breached at this very moment. And many of these companies won't even realize there's an issue until mounds of data have been compromised. You can't possibly assess whether or not your vendor's security is in order unless you have access to their network in real time. But if you use a continuous monitoring solution like BitSight, you can take action against real threats immediately.

Want to see BitSight in action with a free demo?

It's easy. **Click here to get started.**

Learn how forward-thinking companies are handling risk management with technology.

Security ratings could completely revolutionize how your company is handling risk management.

http://www.bitsighttech.com

WHITE PAPER

Making Risk Management

DOWNLOAD WHITEPAPER >

vith

Ratings

April 2014