Rules to Receive CPE Credit

By attending today's session, you are eligible to receive 1 CPE Credit per the following guidelines:

In order to receive this credit, the following items MUST be completed:

- ✓ Each person wishing to receive CPE Credit must log into the session individually with their credentials
- ✓ You MUST answer ALL of the polling questions throughout the presentation
- ✓ You MUST be in attendance for the entire live session
- ✓ You MUST complete the follow-up survey regarding the session

venminder

Vetting Your Vendor's Cybersecurity Preparedness

PRESENTED BY
Lisa-Mae Hill

Information Security Operations Manager
Venminder
lisa-mae.hill@venminder.com

October 12, 2021

Session Agenda

1

What is vendor cybersecurity posture and why it's important

2

What vendors should be reviewed and when

3

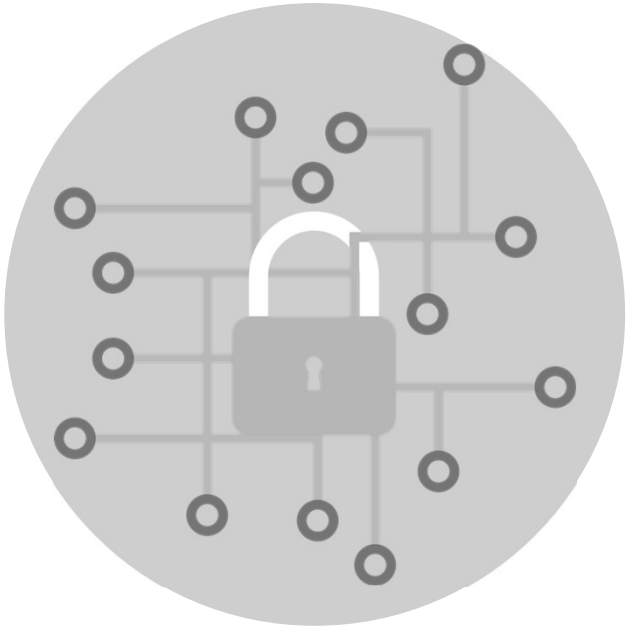
Top 4 areas of vendor cybersecurity to review

venminder

Vendor Cybersecurity Posture

Is your vendor prepared to prevent, detect and respond to a cybersecurity issue?

- Identify the cyber threats your vendor could present and take proactive steps to mitigate potential areas of weakness
- Ensure you determine if your vendor (and your customers' data) will be secure
- Review if your vendor is prepared to prevent, detect and respond to a cybersecurity issue

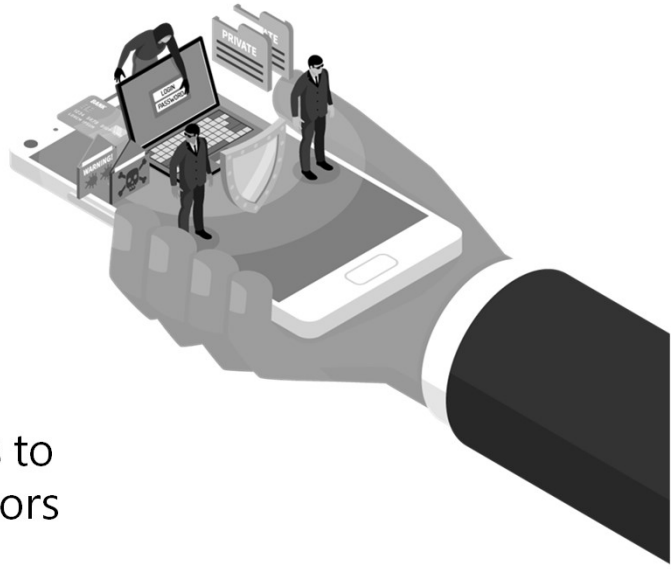


venminder

Why It's Important

Enables your risk mitigation by allowing you to:

- Influence the vendor to strengthen their controls
- Supplement their controls with controls of your own
- Make a decision on whether you should stay with the vendor



It's a hot button issue for all regulators!

- It's required that you demonstrate you are taking proactive steps to identify and mitigate potential areas of weakness with your vendors
- Expected to cover the CIA Information Security Triad

venminder

Notable 2020-2021 Vendor Data Breaches

- **SolarWinds** – Serving as a vendor for more than 300,000 customers, the enterprise monitoring software provider's breach is one of the worse beaches to date. To this day, it's still under investigation.
- **Colonial Pipeline** – The fuel supplier had to proactively close down operations and freeze IT systems due to cyberattack caused by a compromised employee password.
- **Blackbaud** – The third-party cloud computing vendor experienced a breach that exposed the information of millions of healthcare patients.
- **Zoom** – The video conferencing vendor experienced security issues and vulnerabilities in 2020 with the surge of platform use.
- **Accellion** – A security flaw in their software vendor led to a data breach that is impacting its users affecting more than 2.7 million (e.g., universities, banks and more).

Privacy Laws

3 States have comprehensive privacy laws (Only CA currently in effect)

- **California**: 2 of them
  - California Consumer Protection Act (CCPA)
    - Went into effect: Jan 2020
  - California Privacy Rights Act (CPRA)
    - Going into effect: Jan 2023

- **Virginia**: Virginia Consumer Data Protection Act (CDPA)
  - Going in effect: Jan 2023

- **Colorado**: Colorado Privacy Act (CPA)
  - Going in effect: July 2023

venminder

Why It's Important

The Domino Effect Is Real

A chain is only as strong as its weakest link

venminder

Poll Question

When do you perform a cybersecurity assessment on a vendor with access to consumer data or your systems?

a. Pre-contract signing and annually thereafter as a part of vendor management
b. Post-contract signing as a part of vendor management
c. When resources are available
d. Cybersecurity is not included as a part of our due diligence or vendor management process
e. Not sure

venminder

The CIA Information Security Triad

Cybersecurity is based on the CIA Information Security Triad that encompasses:

Confidentiality – seeks to prevent unauthorized disclosure of information

Integrity – seeks to ensure that data is not modified by unauthorized means

Availability – ensure that information is available when needed and only to authorized personnel

venminder

What Vendor's Cybersecurity Should Be Assessed & By Whom

What type of vendors should be assessed?

- All moderate, high and critical risk vendors
- Any vendors that process, store or transmit your data

Who at your organization should assess 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

venminder

When Should You Assess?

Due diligence and residual risk determination

Ongoing monitoring and oversight

venminder

Poll Question

How many of your third-party contracts require incident notification parameters?

a. All
b. Some
c. Only critical or high-risk vendors
d. None
e. Not sure

venminder

Protection Inside Vendor Contracts

- ✓ Accessibility to the vendor's cyber policies and procedures
- ✓ Independent testing requirements
- ✓ Frequency and availability of test results
- ✓ Recovery times
- ✓ Back-up responsibilities
- ✓ Cyber resilience
- ✓ Management of third-party/outsourced business continuity
- ✓ Breach/disruption notification

venminder

What to Review: 4 Critical Elements

1. Security Testing
2. Sensitive Data Security
3. Employee, Contractor and Vendor Management
4. Incident Detection and Response (and Cybersecurity Insurance Coverage)

venminder

Security Testing

Testing is one of the best ways to identify weaknesses. Request your vendor perform the following at least annually:

- ✓ Internal and External Vulnerability Testing
- ✓ Penetration Testing
- ✓ Social Engineering

venminder

Sensitive Data Security

If information needs to be protected against unintended disclosure, then you should be aware of how the vendor is protecting the data from destructive forces and from unwanted actions of unauthorized users (e.g., data breaches, theft).

Verify the vendor is taking precautions, such as the following to secure your data:

- Encryption
- Data Retention and Destruction Policies
- Data Classification and Privacy Policies

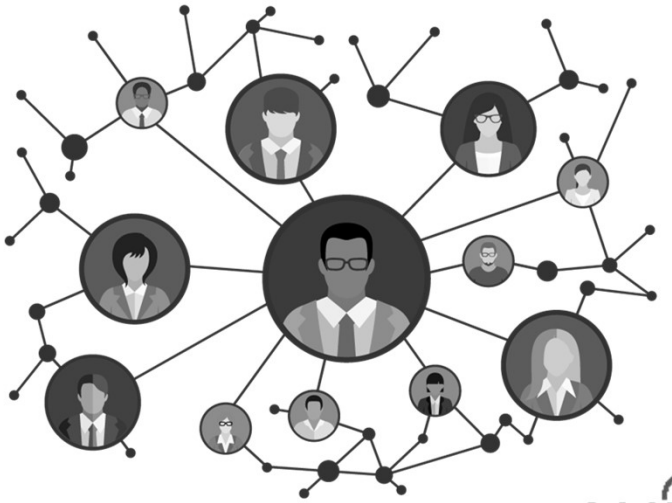
venminder

Employee, Contractor & Vendor Management

Understand the vendor's ability to ensure their employees, contractors and vendors (your fourth parties) are prepared to protect data that is crucial to their overall cybersecurity.

Review the following and confirm they're adequate:

- Confidentiality Agreements
- Security Training
- Access Management Policies



venminder

Incident Detection & Response

An incident is anything that affects the confidentiality, integrity or availability of information or an information system. A vendor should have a plan to address an incident quickly and effectively when (not if) one happens.

Understand how a vendor handles incident detection and response by:

- Including incident notification clauses within your contract
- Reviewing the incident management plan to ensure it's comprehensive
- Verifying the vendor has cybersecurity insurance coverage

venminder

Your Vendor Has Been Breached…What's Next?

(IT'S NOT IF, IT'S WHEN)

- Ensure data breach notification requirements are documented in your contract language
- Set expectations with your vendors
- Define the impact of the breach
- Be transparent
- Adopt a customer notification process

In-house:

- Assess your own overall information security processes
- Implement more robust user authentication procedures
- Restore customer faith

venminder

Poll Question

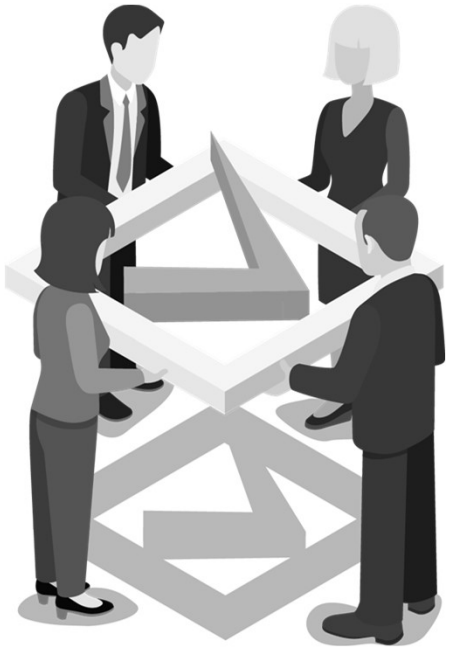
Was your organization a victim to any recent data breaches?

a. Yes
b. No
c. Somewhat
d. Not sure

venminder

Remember the following:

1. Security Testing
2. Sensitive Data Security
3. Employee, Contractor & Vendor Management
4. Incident Detection & Response (also Cybersecurity Insurance Coverage)



Questions & Answers

Post a Question:

www.thirdpartythinktank.com

THIRD PARTY thinktank
A Community for Risk Professionals

Email Us:

lisa-mae.hill@venminder.com

Follow Us:

@venminder

venminder

Also Join Us At
Our Upcoming Webinars:

OCTOBER 26, 2021
Understanding and Analyzing Vendor SOC Reports

NOVEMBER 9, 2021
Vendor Risk Assessment Workshop

Click here to view our Webinars Page.

venminder

Thank You