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 Director
Venminder
lisa-mae.hill@venminder.com

October 18, 2022

Session Agenda

1. Why vendor cybersecurity preparedness is important
2. What vendor should be reviewed and when
3. What to review
4. Recent breaches

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
- You're expected to cover the CIA Information Security Triad

venminder

Notable 2022 Vendor Data Breaches

CommonSpirit Health

- In October, one of the largest hospital chains in the U.S. was hit with a suspected ransomware cyberattack last week.
- This ultimately led to a delay in actual medical care including surgeries, hold ups in patient care, and the need to immediately rescheduled doctor appointments across the country.
- CommonSpirit is the fourth-largest health system in the country. The attack forced it to take certain systems completely offline. Though specifics have yet to be shared, an insider has stated that they had sustained a ransomware attack.

Oktapus Phishing Breach

- In August, the cybersecurity company, Group-IB, detailed a months-long phishing campaign that compromised at least 130 companies, including Cloudflare, DoorDash, Mailchimp, and Twilio.
- The attack was executed primarily by imitating the authentication service Okta. Via text message, they would direct their targets to a fake authentication page, where the victims would then enter their login credentials, giving the attackers access to their account.
- These attackers would use one compromised service to breach another. For Instance, they leveraged their access to Twilio's phone number verification services to attempt to compromise 1,900 signal users.

Notable 2022 Vendor Data Breaches

Twitter

- In July, a hacker using the alias ‘Devil’ posted on that they had obtained personal data on 5.4 million Twitter users, including email addresses and phone numbers.
- ‘Devil’ had apparently exploited a vulnerability to scrape this data from Twitter and posted it for sale with an asking price north of $30,000.

Microsoft

- The hacker group LAPSUS$ posted a screenshot to their Telegram channel indicating that they had breached Microsoft.
- In March, the screenshot was taken within Azure DevOps, a collaboration software created by Microsoft, and indicated that Bing, Cortana, and other major Microsoft projects had been compromised in the breach.
- This is still under investigation and unclear if any personal or account information has been exposed or leaked.

Privacy Laws

5 States have comprehensive privacy laws (Only California is currently in effect)

1. **California:** 2 of them
    - California Consumer Protection Act (CCPA)
        - Went into effect: January 2020
    - California Privacy Rights Act (CPRA)
        - Going into effect: January 2023
2. **Virginia:** Virginia Consumer Data Protection Act (CDPA)
    - Going into effect: January 2023
3. **Colorado:** Colorado Privacy Act (CPA)
    - Going into effect: July 2023
4. **Utah:** Utah Consumer Privacy Act
    - Going into effect: December 2023
5. **Connecticut:** Connecticut Data Privacy Act
    - Going into effect: July 2023

Helpful legislation tracker: *https://iapp.org/resources/article/us-state-privacy-legislation-tracker/*

venminder

Why It's Important

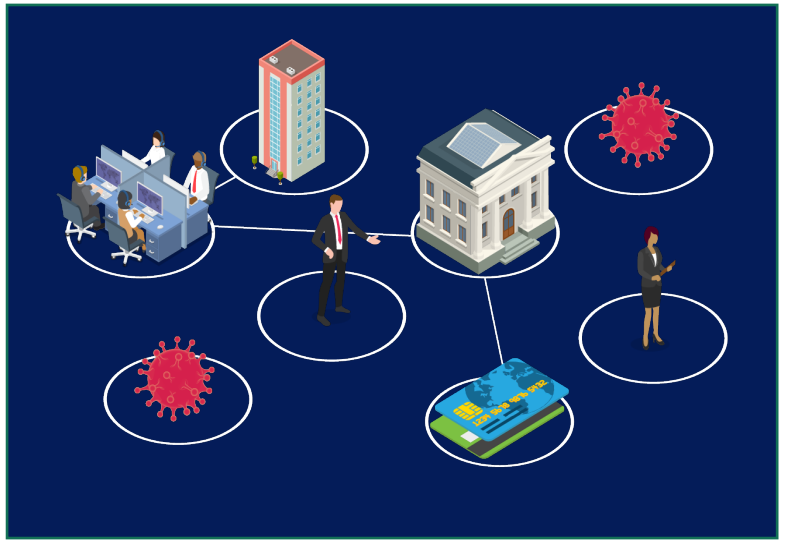
The Domino Effect Is Real

A chain is only as strong as its weakest link

venminder

Cybersecurity Post Pandemic

- **Working remotely created new loops for cybercriminals to exploit**
  - Remote workers often lack secure equipment and protocols that provide robust digital controls and compliance
  - Organizations are continuing to embrace the remote workforce
  - Increased reliance on cloud-based communication
  - Infrastructure AND resources are spread thin
- **Regulators are watching**
  - How are you handling these ongoing risks?
  - How are you ensuring your VENDORS are handling the risks?



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 isn't included as a part of our due diligence or vendor management process
e. Not sure

venminder

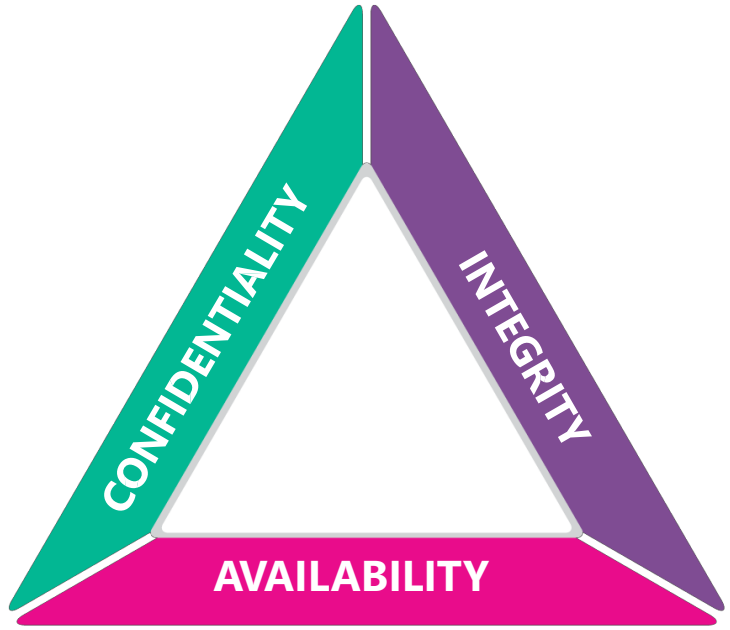
The CIA Information Security Triad

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

Which Vendors 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

When Should You Assess?

Onboarding: During planning & risk assessment and due diligence before contracting

Ongoing: During re-assessments, monitoring & performance, renewals, and due diligence

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, and 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:

- Pre-Contract Vendor Due Diligence & Ongoing Vendor Monitoring
- Security Training
- Background Checks
- Access Management Policies

venminder

Incident Detection and 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

Your Vendor Has Been Breached…What Next?

The most common repercussions of a vendor data breach are:

- Increased regulatory scrutiny
- Possible fines or other monetary impact
- Loss of customer confidence
- Reputational damage

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

venminder

Your Vendor Has Been Breached…What's Next?

In-house:

- Determine *how* it happened
- Re-evaluate the vendor relationship
- 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, and Vendor Management
4. Incident Detection & Response (also Cybersecurity Insurance Coverage)

Best Practices

1. Right to Audit language in contracts
2. Only share sensitive data when necessary
3. Ask for everything you'll need upfront
4. Make sure you know who to review and when
5. Ensure you have the right people doing the review
6. Understand what data you are trying to protect
7. Always include breach notification language in your contracts
8. Be prepared with your own breach notification plan
9. Be as proactive as you can, but be ready to be reactive

venminder

Thank You

Also Join Us At
Our Upcoming Webinars:

Today at 2pm ET
How to Review a Vendor's Cybersecurity Program

OCTOBER 20, 2022
Risk Assessing Your Credit Union's Vendors

Click here to view our Webinars Page.

venminder

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