venminder

Rules to Receive CPE Credit
This live session is eligible for 1 CPE Credit.

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

April 14, 2020

Vendor Cybersecurity Preparedness in a Pandemic World

Presented by Gordon Rudd
Third-Party Risk Officer at Venminder
gordon.rudd@venminder.com

Session Agenda

Securing a completely remote workforce

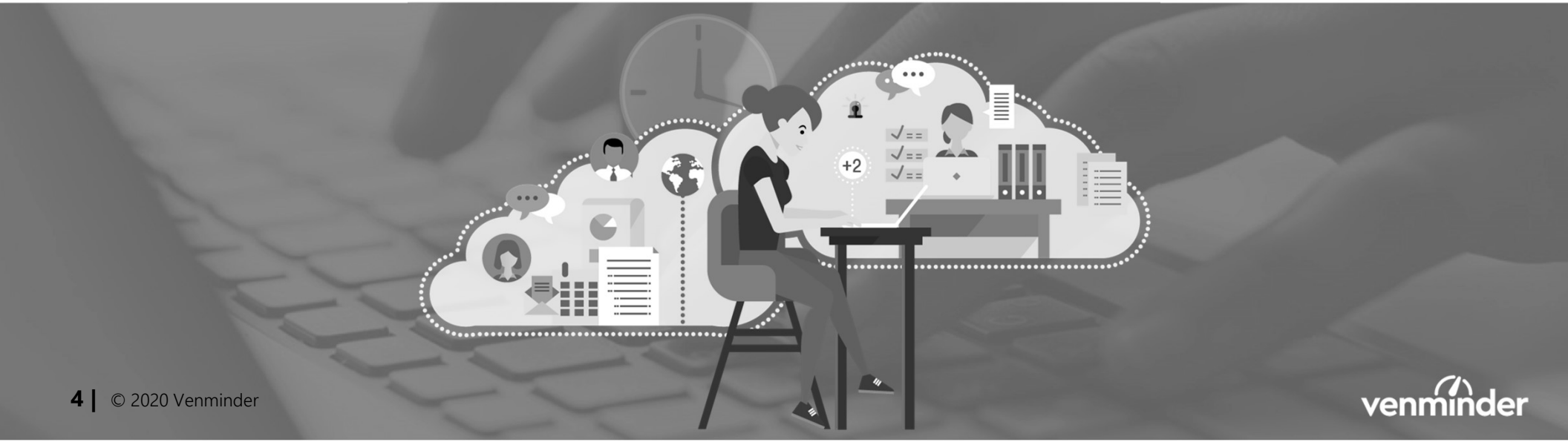
Vendor pandemic planning for cybersecurity

Third-party risk with a **remote workforce**

Best practices to takeaway

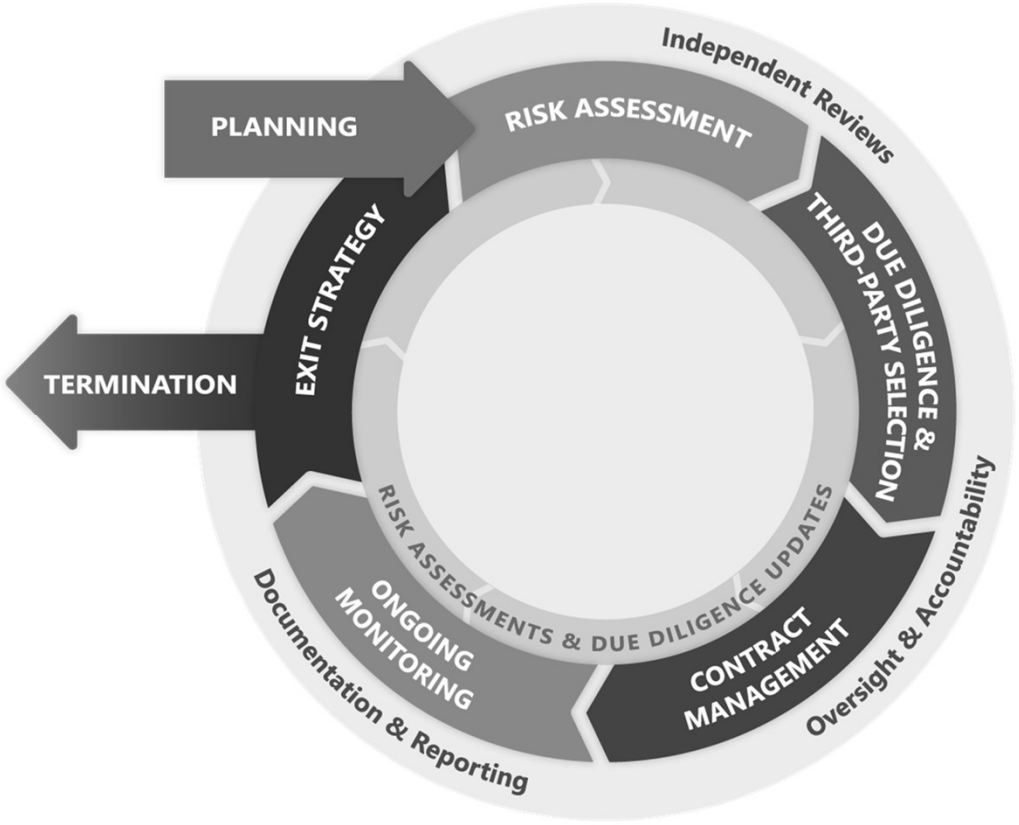
Securing a completely remote workforce

- You invest in understanding your own cybersecurity and must do the same for your vendors
- Understanding your vendors' cybersecurity posture can reduce risk
- Don't let your vendors become your weak link
- Bad actors will still act and likely will increase their activity to prey on the current weaknesses



venminder

Third-Party Risk Management Lifecycle



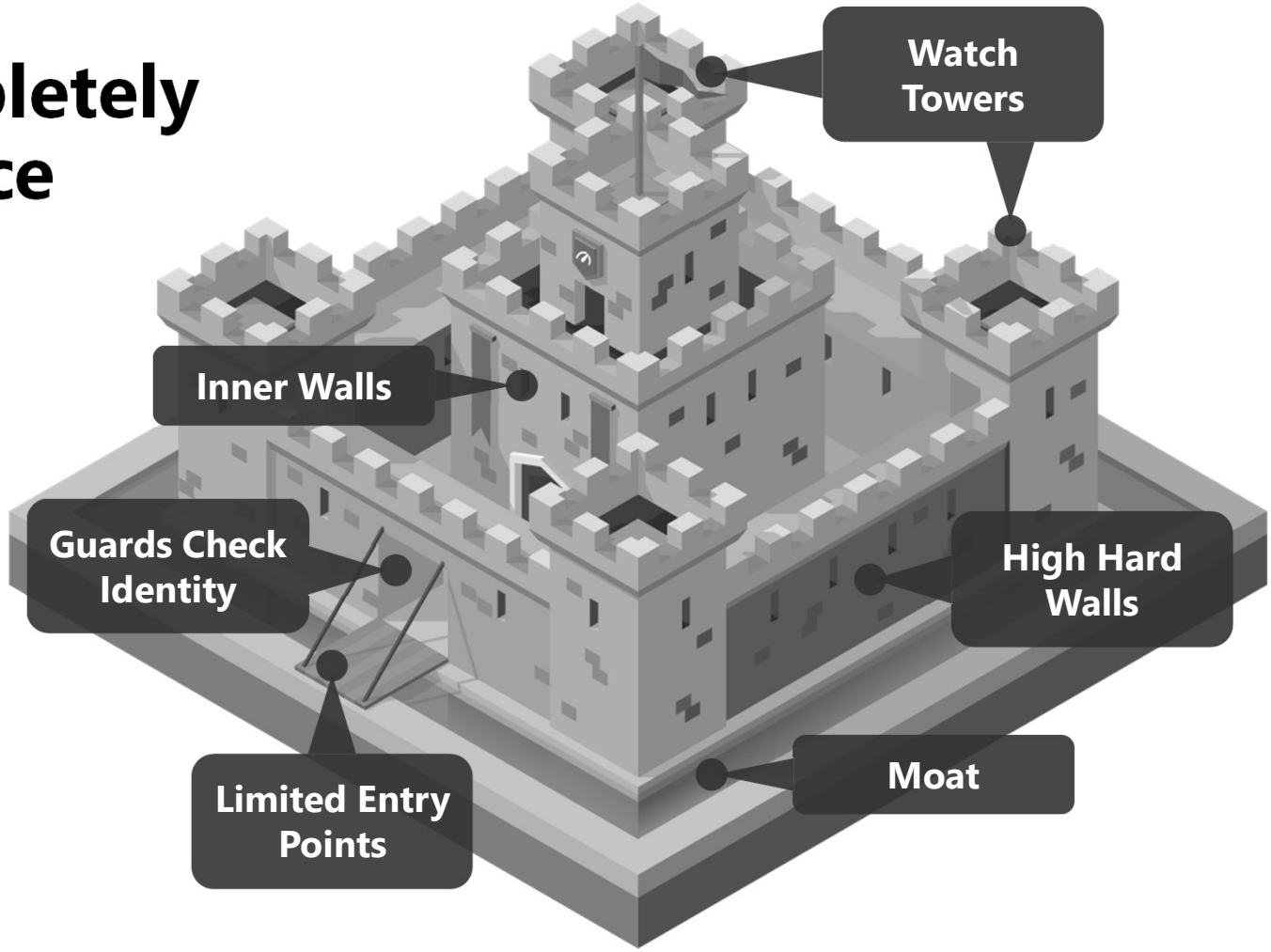
venminder

Cybersecurity Maturity

LEVEL		FOCUS	PROCESS AREA	RESULT
5	Continually optimizing organizational competency	Continuous process improvement is fully operationalized at the enterprise level	• Organizational Innovation and deployment • Causal Analysis and Resolution • Change management competency is evident in all levels of the organization and is part of the organization's intellectual property and competitive edge.	Highest Level of: • cyber assurance • productivity • Quality • Responsiveness & • Profitability
4	Quantitatively managed organizational standards	Selection of a common approach & quantitative management in place	• Organizational process performance • Quantitative project management • Organization-wide standards and methods are broadly deployed for managing and leading change	
3	Defined processes & multiple project capability	Process standardization on best practices is evident	• Requirements Development • Technical solutions • Product integration • Verification • Validation • Organizational process focus & definition • Organizational Training • Integrated Project Management • Risk Management • Decision Analysis and Resolution • Comprehensive approach for managing change is being applied in multiple projects	
2	Managed but isolated projects	Basic project management using many different tactics used inconsistently	• Requirements management • Project planning, monitoring & control • Supplier agreement management • Quantitative measurement and analysis • Process & product quality assurance • Configuration and change management are applied in isolated projects	
1	**INITIAL STAGE** ad hoc or absent • planning • organization • control	Competent People and Heroics People dependent without any formal practices or plans	• Competent People and Heroics • Little or no change management applied	Highest rate of: • project failure • turnover • loss Lowest Level of: • productivity • quality

venminder

Securing a completely remote workforce



venminder

Cybersecurity

for any size corporation – your vendors should have this

1. SETA
2. Who are your stakeholders
3. Watch your numbers
4. Know your 4 P's
   (policy, procedure, process, project)
5. Security architecture
6. Asset ID
7. BCP/DRP
8. Risk Management
9. Training & Cross-training

venminder

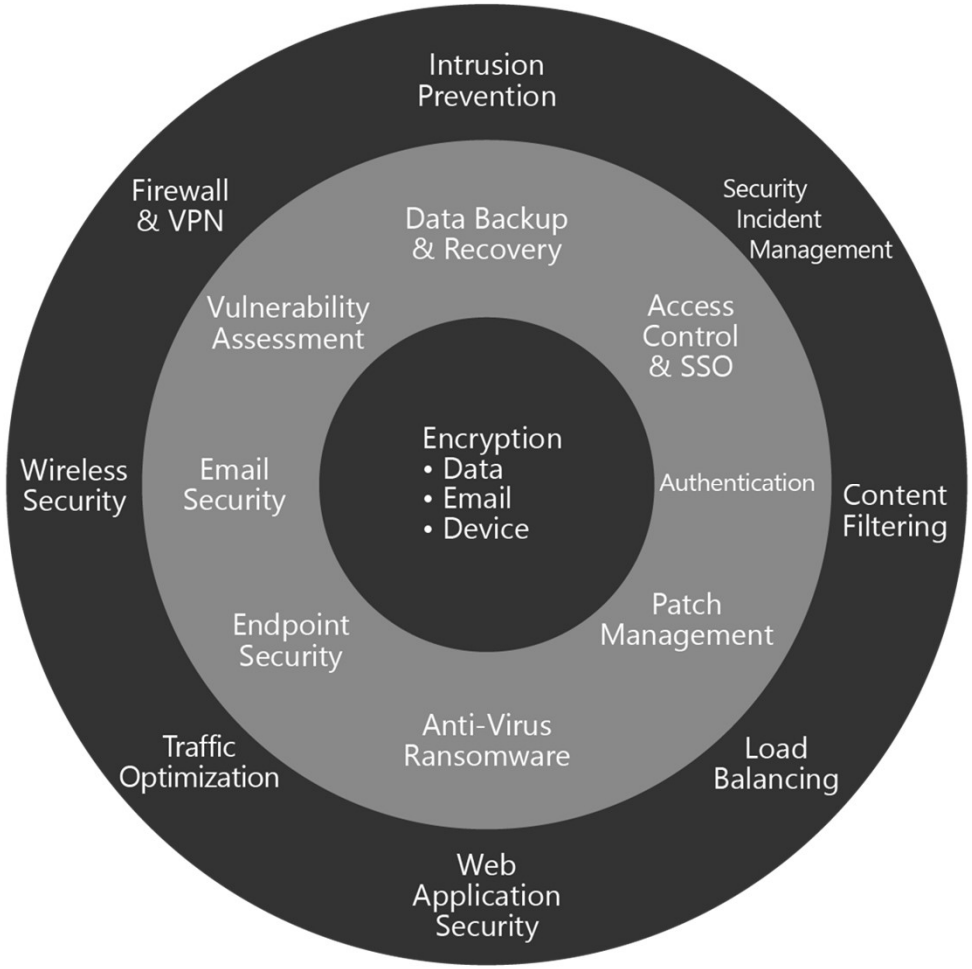
SETA

- What is SETA?
  - Security
  - Education
  - Training
  - Awareness
- Educate your workforce on phishing
- This is a requirement if you have remote employees

venminder

Overlapping Layers

- A standard approach circa 2005-2017
- Today we want to see the AI inside
- This model is your audit baseline



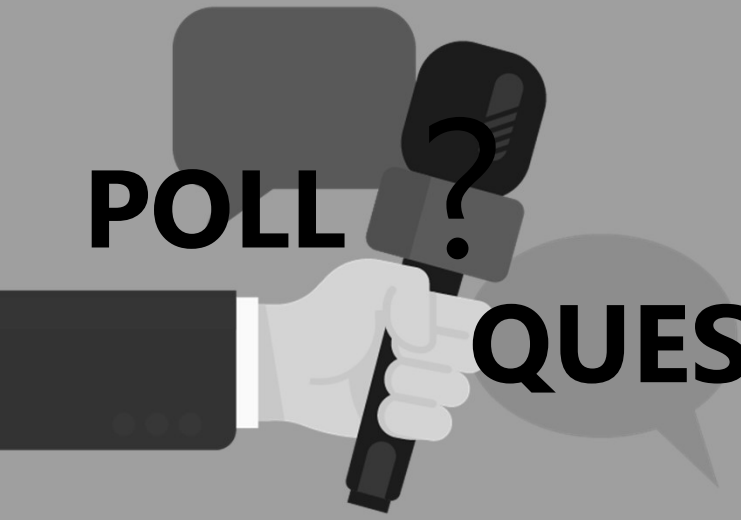
venminder

Vendor Network & Endpoint Defenses

Is your vendor monitoring multiple layers of security like the following?

- Firewalls
- Data Loss Protection
- Spam Filtering
- Antivirus
- Threat Emulation
- HTTPS Inspection
- Bot Protection
- Application Control
- URL Filtering

venminder



Do you review & assess your critical and high-risk vendors' cybersecurity plans?

a. Yes – 100% of critical and high-risk vendors
b. Only for critical vendors
c. Only for high-risk vendors
d. No – Never
e. Not sure

venminder

Is it **enough?**

- Nothing is foolproof
- There is no magic bullet
- With enough time and money, anything can be breached
- Users make mistakes
- Vendors make mistakes

venminder

What they don't see can kill them

Continue to be on high-alert

Watch for These:

- Brute force attacks on all assets
- Brute force on local accounts
- Detection evasion – local event log deletion
- Privilege escalation
- Lateral movement
- New local user accounts created
- Protocol poisoning
- Failure to mitigate these risks could result in a data loss or breach

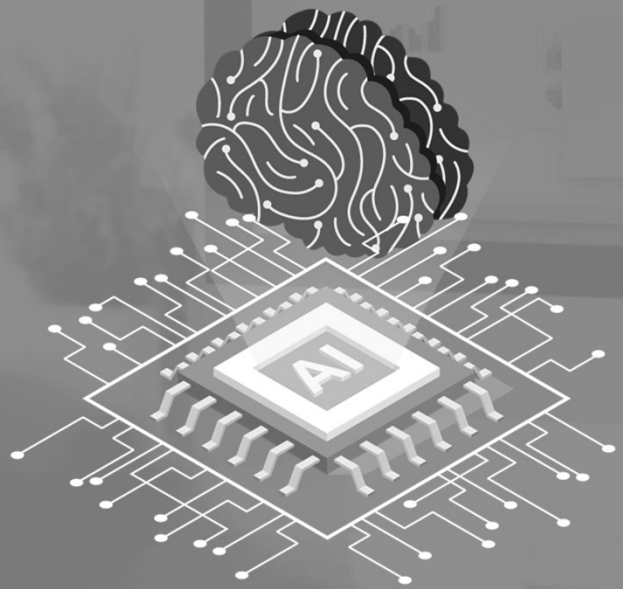
venminder

How do the vendors gain insight?

- Artificial Intelligence?
- Machine Learning?
- Cluster Algorithms?
- Additional Staff?
- Specialized Applications?

venminder

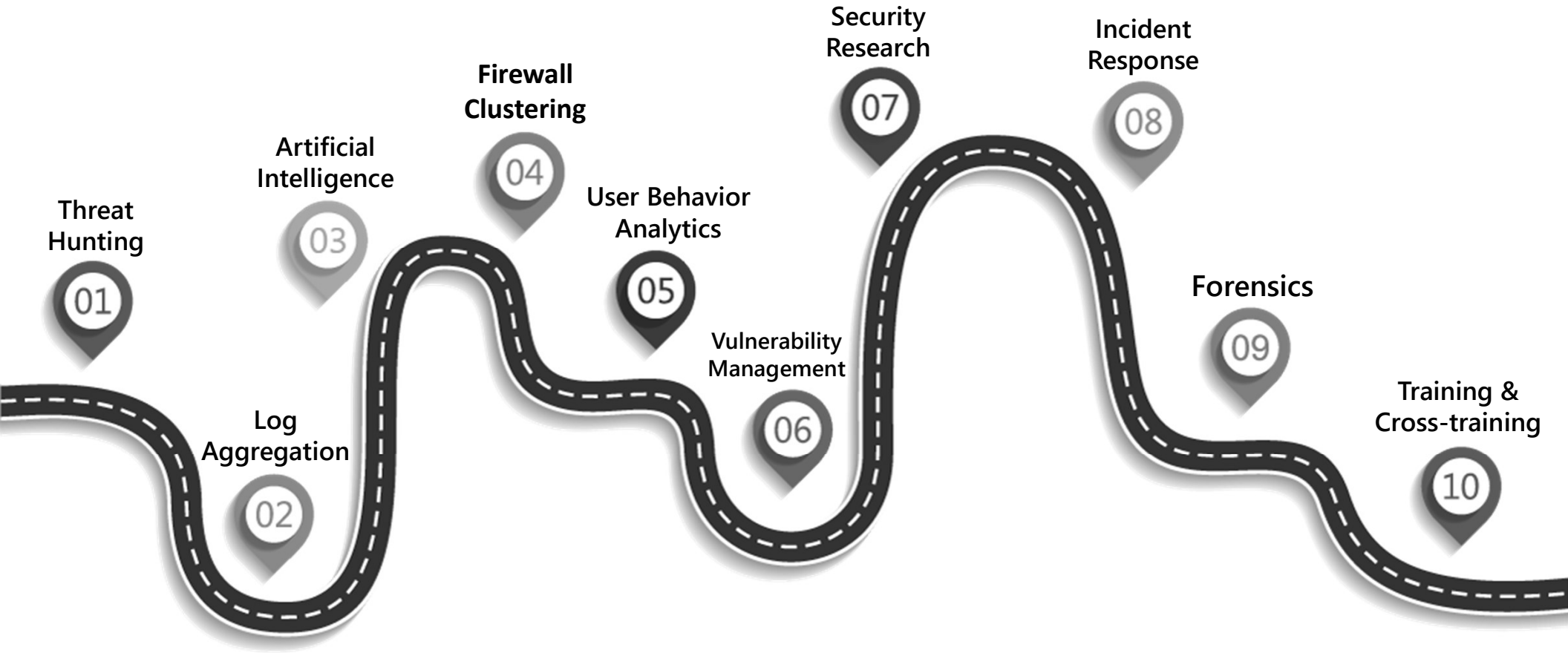
AI & Behavioral Analytics



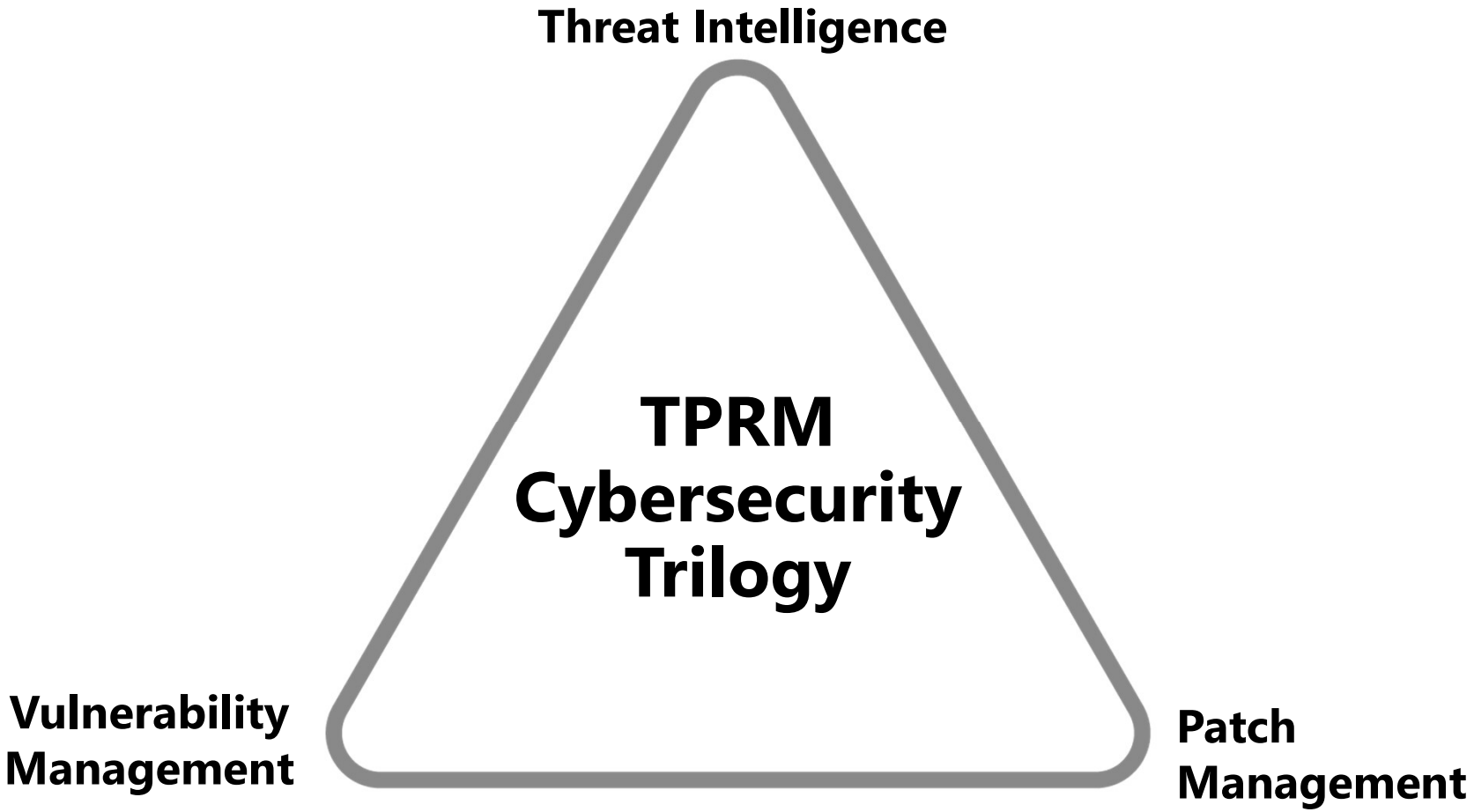
- Learns what your network traffic looks like
- Connects the dots from all the many, many logs
- Detects the anomalies that look like legitimate traffic
- Exposes intruders
- We see all the water molecules in the flowing river

venminder

Cybersecurity Road Map Documentation



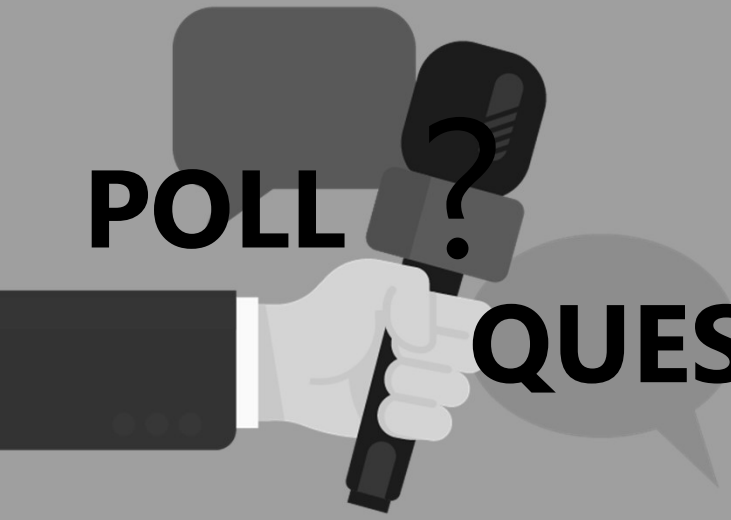
venminder



Most Common Cybersecurity Mistakes You Want Your Vendors to Avoid!

1. Thinking it won't happen to you. The one thing people absolutely must understand is that hackers are not picky
2. No SETA program
3. Thinking it's just about malware
4. Not monitoring
5. Not learning the basics
6. Failing to locate data
7. Not testing the security
8. Ignoring training
9. Not assessing vendor risks
10. Failing to map data flows AND lives
11. Concentrating too much on the perimeter
12. Overlooking "Shadow IT"
13. Failing to work closely with your stakeholders
14. Resisting vendor risk assessments

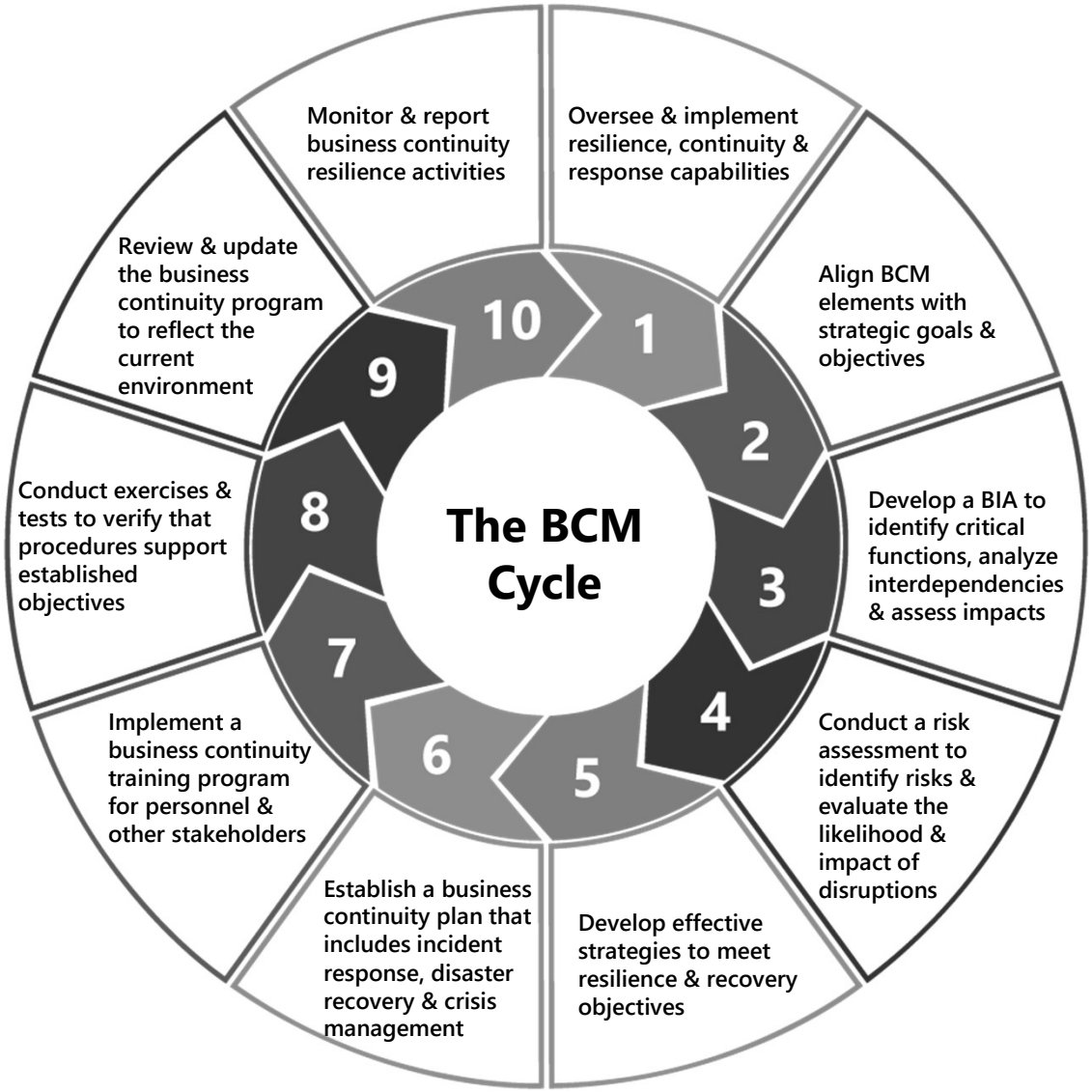
venminder



How often do you ask your critical and high-risk vendors for copies of their cybersecurity plans?

a. Annually
b. When first vetting the vendor
c. Depends upon the vendor's level of risk and criticality
d. Never
e. Not sure

venminder



venminder

Pandemic Planning

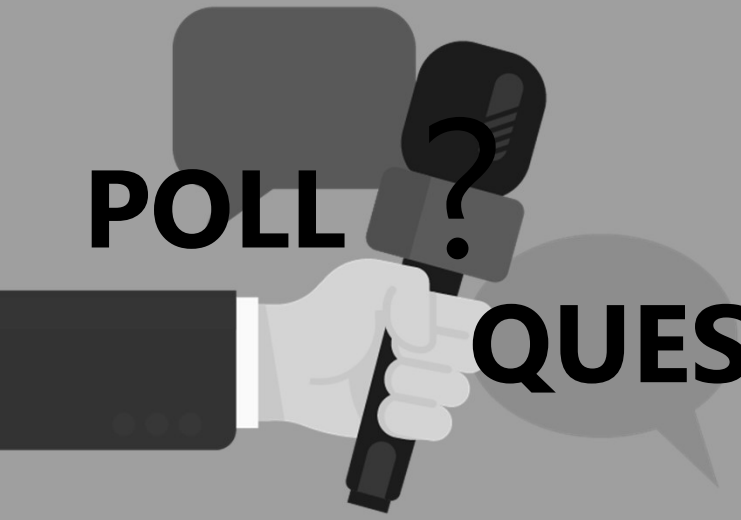
- A pandemic plan bridges the gap between business continuity planning and disaster recovery
- It is a living document, setting forth your strategies, procedures, preventative measures, declaration point and guidelines an organization will take should a global health crisis occur
- What does your vendor's pandemic plan will tell you?

venminder

Vendor Pandemic Planning for Cybersecurity

1. **Current BCM plan + pandemic plan**
2. **MDM policy + connectivity standards**
    a. Remote workforce guidelines for data
    b. Personal device management guidelines
        i. End point protection & patch management
3. **Ongoing employee education**
4. **BCM**
    a. Incident Response
    b. Crisis Management plans include 100% remote workforce

venminder



Do you review & assess your vendors' business continuity management (BCM) plans?

a. Yes – 100% of critical and high-risk vendors
b. Only for critical vendors
c. Only for high-risk vendors
d. No – Never
e. Not sure

venminder

Business Impact Analysis (BIA)

Ask Yourself:

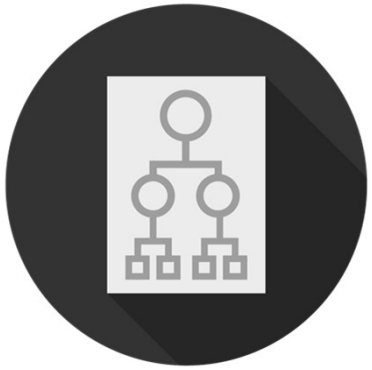
- Would a sudden loss of this vendor cause a material disruption to my organization?
- Would that sudden loss of this vendor impact our customers?
- Would the time to recover be greater than one business day or greater than what your business continuity plan calls for as a recovery time?

- **BIA: An analysis to determine if your organization can operate effectively while the vendor is unavailable.**
- **During business impacting events like pandemics, your vendors are more vulnerable (breach, phishing attacks and other cyber crimes) that may affect operations**
- **Your BIA should be reviewed if there is updated regulatory guidance or when significant change occurs within your organization or the vendors.**

venminder

Identification of Critical Business Functions

The BIA must include critical business functions, including support activities (e.g., help desk, call center, human resources and payroll), systems, and interrelationships may be analyzed in several ways.



Workflows, interviews, organizational charts, network diagrams/topologies, data flow diagrams, succession plans, or delegations of authority for key personnel may help management identify business processes and hierarchies.

venminder

Best practices for vendor cybersecurity to keep your organization safe

1. Make sure your vendors have a SETA program
2. Watch your vendors' firewall numbers to verify they can respond accordingly
3. Know your vendors' 4 P's - policy, procedures, process and project
4. Understand the vendors' security architecture
5. Make sure vendors are identifying the asset IDs on their network
6. Ensure vendors have a business continuity management plan
7. Incorporate cybersecurity in risk management processes for critical and high-risk vendors
8. Verify vendors are providing cybersecurity training & cross-training

Question & Answer

Follow us on:

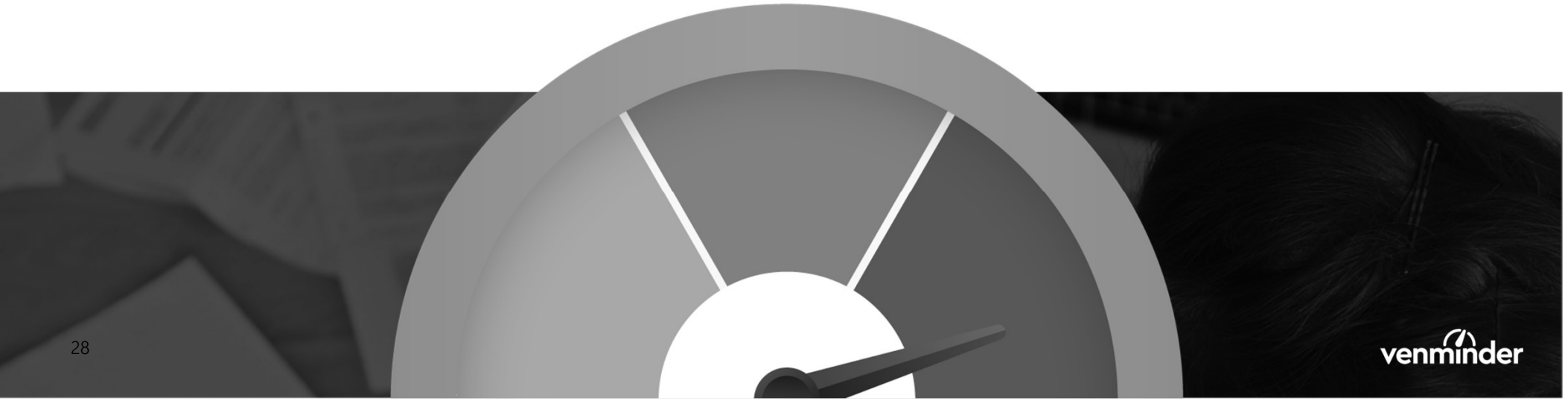
@venminder

venminder.com

thirdpartythinktank.com

Join the conversation:

THIRD PARTY thinktank



ALSO JOIN US AT
Our Upcoming Webinars:

April 21 – 23, 2020
Third-Party Risk Management Bootcamp

May 12, 2020
Vendor Complaints: A Cause for Enforcement Actions

Click here to view our Webinars Page.

Thank You

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

venminder.com

thirdpartythinktank.com

Follow us on:

Join the conversation in:

THIRD PARTY thinktank