Is Your 3rd-Party Risk Program Ready for the Next Supply Chain Crisis?

Brenda Ferraro
Vice President, Third-Party Risk
Prevalent

Steve Roesing
CEO
ASMGi
Your Presenters

Brenda Ferraro
VP, Third-Party Risk
Prevalent

Steve Roesing
President, CEO
ASMGi
Agenda

Accelerating procurement and sourcing

Expanding sources of vendor risk intelligence

Working with suppliers to proactively reduce risk and ensure compliance

Driving more informed, risk-based decision making across your organization
What are the challenges with accelerating procurement and sourcing?
Procurement & Sourcing

Supply Chain Universe
Visibility on all vendors IT, OT, Manufacturing, Transportation, etc.
Govern and manage the supply chain lifecycle from onboarding to termination
Develop a preferred supply chain list of vendors with mature security and resiliency

RFx & Selection
Provide rapid information using threat intelligence
Use the scoring and thresholds to provide risk scoring as part of the overall segmentation
Receive information on maturity acumen prior to selection

Profiling & Context
Capture context on supply chain and outsourcing chain engagements for proper due diligence
Create tags and identifiers for reporting to account for relationship mapping
Sets up tiering and prioritization

Inside Out & Outside In
Gather and normalize responses via questionnaires and threat intelligence to identify true risk
Provide ongoing and continuous evaluation intelligence as risks are identified, monitored and mitigated
Are you seeing an expansion in the sources of vendor risk intelligence?
Efficiency, Visibility and Scale

Manual
- Juggle emails, spreadsheets, and SharePoint

Network
- Leverage a vendor risk management solution to automate assessments of internal controls

Unified
- Access a repository of pre-completed assessments and risk scores
- Validate data from internal controls assessments with external, continuous cyber and business risk monitoring

Integrated
- Bridge technology silos; share context and intelligence
- Proactively and continuously assess, monitor and eliminate vendor risks – before they impact the business

Discover
- Assess
- Analyze
- Remediate
- Optimize
Add Speed and Scalability with the Vendor Intelligence Network

**Global Vendor Intelligence Network**

**Research Intelligence**
- Extended Profile
- Cyber & Breach Monitor
- Business & Certifications Monitor
- Third Party Connectors

**Community Intelligence**
- Verified Assessments
- Vendor Events
- Community Analytics
- Member Events

Assessment Libraries Add Speed and Scale

**Vendor Community**
- Proactive assessments
- Certifications
- Docs & agreements
- Events

**Vendor Risk Intelligence**
Continuous, comprehensive, relevant:
- Global research
- Assessments
- Partner feeds

**Completed Assessments**
- 10,000+ verified records
- Sig-Lite/Sig-Core
- Prevalent Compliance Framework (PCF)
- Cybersecurity Maturity Model Compliance (CMMC)

**Private Sources**
- Credit reports
- Risk scores
- Financials
- Payments
- Legal Actions
- Certifications
- 65+ threat feeds
- 50+ paste sites
- Blogs & social media
- Code repositories
- 1.5k+ hacker forums
- Dark web (80+ forums)

**Technology Integrations**
- ServiceNow
- RSA Archer
- BitSight
- And more

**Regulatory Monitoring**
Coverage across 15+ regulations and frameworks:
- CAIQ
- CMMC
- GDPR
- HIPAA
- ISO
- PCI
- NYDFS
- And more

**Public Sources**
Business & breach monitoring across 200k+ sources
- Data breach sites
- Corporate sites
- News feeds
- Trade publications
- Industry sites
- And more

**Industry Partnerships**
- H-ISAC
- LVN
- Legal Theorem
- Shared Assessments

**Completed Assessments**
- Prevalent Compliance Framework (PCF)
What techniques work well to proactively reduce risk and ensure compliance?
Entity Profiling

Review a Comprehensive Profile of Risk, Compliance, and Context on a single page for vendors or internal business functions. Profile Data is importing from the Intelligence Network and/or connected system integrations.

- **Risks** captured from assessments and automatically translated from monitoring feeds.
- **Compliance** correlated from predefined or custom mappings against domains.
- **Context** regarding what they do and how collated from business feeds and verified by entity owners.
Assessment Insights

Assessments drive automatic risk identification and give insight into policy and process. Proactive Assessments allow for regular and opportunistic information gathering, including event management. Assessment Insights can be importing from the Intelligence Network and/or from launching vendor assessments using automation playbooks.

Scheduler allows regular assessments and chasers to entities from a broad range of library assessments.

Auto Inherent/Residual Risk identified automatically from every assessment, factoring ongoing management.

Self-Reporting ability for entities to report an event which requires action.
Continuous Monitoring Insights

Continuous Monitoring includes Cyber, Business, and Financial Events synchronized daily. External feed data can provide actionable intelligence. Monitoring Insights can be importing from the Intelligence Network and/or from enabling continuous monitoring using automation playbooks.

- **Actionable** through automatic risk creation, tasks, and review flags.
- **Reportable** through either the Platform risk reporting, or via generated PDF reports with executive summaries.
- **Contextual Mappings** through risk relationships which correlate results to assessment, audit, or compliance findings.
Normalized Risk Insights

All Data is Normalized as **Risks**, providing a mechanism for consistent remediation, reporting, and analytics. This feeds into an AI/ML analysis engine for powerful insight. Risks are quantified and infused with additional context and relationship mapping.

- **Automatic Creation** of risks from continuous monitoring, profiling, and assessments.
- **Guided Remediation** via proposed actions, task allocation, and automated status changes.
- **Contextual Associations** through risk relationships, providing context and compensating controls.
Program Playbook Automation

**Automation Libraries** provide custom or default templates that can be linked into playbooks to enable the automation of program functions such as onboarding, assessment distribution, monitoring enablement, risk triage, risk remediation, and approvals.

- **Granular Triggers** mean automatic workflows can be created for any customer use case.

- **Risk Modification** can be automated based on the entity, for example Tier 1s are prioritized, or monitoring results correlated against assessment results.

- **Human Triggers** allow users to validate the automated workflow for audit trails.
Aggregated Reporting Insights

**Machine Learning/ AI Reporting** through customized dashboard and notifications. Reporting and Analytics on workflow progress, assessments, monitoring, risks, and user behavior.

- **Customized Dashboards** leverage a library of templates built for different program role requirements.

- **Exception Identification** integrated machine learning automatically highlights any results or user behavior which does not conform to normal activity.

- **Automated Insights** show any identified trends or examples of entities which require additional focus.
Are there unconventional ways to drive more informed, risk-based decisions across an organization?
How to Visualize the Full Risk Picture

Focuses on driving a common workflow, providing automation to accelerate the program while delivering actionable insights. This is provided through comprehensive profiles of entities.
### Powerful Capabilities at Every Stage of TPRM Maturity

#### Stop the Pain

<table>
<thead>
<tr>
<th>Traditional Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standardized Questionnaires</td>
</tr>
<tr>
<td>50+ Standard Assessments</td>
</tr>
<tr>
<td>Custom Assessments</td>
</tr>
<tr>
<td>Proactive &amp; incremental assessments</td>
</tr>
<tr>
<td>Automatic risk creation</td>
</tr>
<tr>
<td>Exec &amp; ops dashboards</td>
</tr>
<tr>
<td>Comments &amp; tagging</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Global Vendor Intelligence Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-completed and verified assessments</td>
</tr>
<tr>
<td>80%+ reduced onboarding time (15 days avg.)</td>
</tr>
<tr>
<td>Continuous cyber monitoring, scoring &amp; alerting</td>
</tr>
<tr>
<td>Deep vendor inspection for profiling, tiering &amp; monitoring</td>
</tr>
<tr>
<td>Proactive and incremental updates &amp; event notifications</td>
</tr>
<tr>
<td>Continuous business scoring from 200k+ sources</td>
</tr>
<tr>
<td>Member intelligence sharing &amp; benchmarking</td>
</tr>
</tbody>
</table>

#### Make Intelligent, Informed Decisions

<table>
<thead>
<tr>
<th>Unified Assessment + Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber monitoring: public sites; deep/dark web</td>
</tr>
<tr>
<td>Business monitoring: financial, legal, brand, etc.</td>
</tr>
<tr>
<td>Risk-based decision-making</td>
</tr>
<tr>
<td>Single view of top risks</td>
</tr>
<tr>
<td>Unified risk register ensures efficiency &amp; consistency</td>
</tr>
<tr>
<td>Inherent &amp; residual risk tracking</td>
</tr>
<tr>
<td>Auto-flagging recommendations</td>
</tr>
<tr>
<td>Automated risk reviews</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Integrated APIs &amp; Connectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce onboarding time by up to 85%</td>
</tr>
<tr>
<td>RESTful API w/ 65+ endpoints &amp; attributes</td>
</tr>
<tr>
<td>Sync vendor profiles and risk ratings</td>
</tr>
<tr>
<td>Connectors for ServiceNow, Archer &amp; Ariba</td>
</tr>
<tr>
<td>Speed communications with workflows &amp; ticketing</td>
</tr>
<tr>
<td>Share risk intel: research, assessments &amp; external feeds</td>
</tr>
<tr>
<td>Consolidate, quantify and analyze threat intelligence</td>
</tr>
<tr>
<td>Report across security, compliance and privacy</td>
</tr>
</tbody>
</table>

#### Adapt & Grow

<table>
<thead>
<tr>
<th>Intelligence-Driven Analytics &amp; Automation Engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-dimensional analysis</td>
</tr>
<tr>
<td>Behavioral analytics &amp; detection</td>
</tr>
<tr>
<td>Uncover hidden risks</td>
</tr>
<tr>
<td>Action enablement</td>
</tr>
<tr>
<td>Rules &amp; actions library</td>
</tr>
<tr>
<td>Vendor attribute &amp; events support</td>
</tr>
<tr>
<td>Extensible engine</td>
</tr>
<tr>
<td>Intelligent actions</td>
</tr>
</tbody>
</table>

---

Stop the Pain

- Make Intelligent, Informed Decisions
- Adapt & Grow
Adopt using a Risk Operation Center (ROC) for support

Provides first- and second-line support for assessment and remediation, addressing queries directly relating to Platform usage and content issued/required.

Comprehensive Support

Entity Management

Full configuration and maintenance of the Platform to maintain health and accuracy.

Onboarding, review and maintenance of entities within the Platform, ensuring points of contact, hierarchy, and attributes remain correct.

Service Delivery

Proactive management of assessments and issuing guidance content to improve response rates. Validation of responses and remediation plan management.

KPI Reporting

Detailed analysis of assessment results and progress, providing simple management information and trends.

Platform Management

Provides first- and second-line support for assessment and remediation, addressing queries directly relating to Platform usage and content issued/required.

Prevalent & ASMGi
Cyber Security – **ONEteam Principles**

**The Old Way: Point-Solution Mindset**
- Reactive
- Focus on Individual Controls
- Fragmented and inefficient
- Spend a lot and not necessarily improve security

**The New Way: Holistic Security Mindset**
- Proactive
- Focus on Total Solutions
- Gap-Based & Risk-Based
- Spend less and improve security more
The Holistic Picture
Risk Intelligence
from Every Corner

Completed Assessments
• Networks & Exchanges
• Sig-Lite/Sig-Core
• Prevalent Compliance Framework (PCF)
• Cybersecurity Maturity Model Compliance (CMMC)

Vendor Community
• Proactive assessments
• Vendor Initiated Events
• Certifications
• Docs & agreements

Vendor Risk Intelligence
Continuous, Comprehensive, Relevant:
• Global research
• Assessments
• Partner feeds

Private Sources
Extended Profiles:
• Credit reports
• Risk scores
• Financials
• Payments
• Legal Actions
• Certifications

Cyber Monitoring:
• 65+ threat feeds
• 50+ paste sites
• Blogs & social media
• Code repositories
• 1.5k+ hacker forums
• Dark web (80+ forums)

Public Sources
Business & Breach Monitoring:
• Data breach sites
• Corporate sites
• Regulatory portals
• Review websites
• Job boards

• Trade publications
• Industry sites
• News feeds
• And more

Technology Integrations
• ServiceNow
• RSA Archer
• And more

Industry Partnerships
• H-ISAC
• LVN
• Shared Assessments
• Legal Theorem

Regulatory Monitoring
Coverage across regulations and frameworks:
• CCPA
• NYDFS
• GDPR
• HIPAA
• ISO
• NIST
• PCI
• CMMC
• CAIQ
• And more

Vendor Community
Vendor Risk Intelligence
Private Sources
Public Sources
Completed Assessments
Risk Validation in a Virtual Only World

Automation Setup
- Questionnaire(s)
- Threat Intel (Cyber & Business)
- Tiering / Profiling
- Key Controls
- Configure Risk Remediation

Include Nth Party Transparency
- Follow the Impact

Use Automated Risk Summary Reports
- Virtual Assessment Scope
- Focus on Highest Risk

Distribute the Final Risk Report
- Communicate Actual Risk Intel
- Provide Risk Remediation Guidance

Conduct the Virtual Assessment
- Plan / Do / Check / Act
- Set up View Access Rights

Harmonize the Risks
- Trust (Questionnaire)
- Verify (Threat Intel)
- Validate (Virtual Assess)

Continuously Evaluate & Report
- Track Risks to Closure
- Adjust Risk based on Triggered Events
- Reflect Status on KRI & KPI Reports
Questions?

- info@prevalent.net
- Follow Prevalent on LinkedIn
- Follow Prevalent on Twitter

- info@asmgi.com
- Follow ASMGi on LinkedIn
- Follow ASMGi on Twitter