Automating Supply Chain Risk Incident Actions and Response

18th March 2021

Today's Agenda

1   Introductions

2   Growing Risks & Challenges in the Supply Chain

3   Building A More Responsive Model for TPRM

4   Q & A

Your Expert Panel

John Bree

Chief Risk Officer & Chief Evangelist

Supply Wisdom

Sean O'Brien CTPRP, CTPRA

Managing Director

DVV Solutions

Interconnected Ecosystems - Global & Industry Supply Chains

- Supply chains are increasingly complex

- A route into well protected enterprises

- Historical focus on Tier 1 & 2 suppliers

- Point-in-time assessments can't keep pace

- Limited in-house resources & skills

Diagram from Deloitte Supply Chain & Digital Analytics Survey 2019

Global shipping thrown into 'chaos'

Why workers in some countries are more comfortable about returning to the office

Half of UK manufacturers exposed to supply chain risk as COVID-19 derails Brexit planning

71% of Employees Globally Admit to Sharing Sensitive and Business-Critical Data Using Instant Messaging and Business Collaboration Tools,

How the SolarWinds hack and COVID-19 are changing cybersecurity spending

Covid: 'People are tired of working from home'

5 MAR 2021 NEWS

SITA Supply Chain Breach Hits Multiple Airlines

Outsourcing and third party risk management

Consultation Paper 30/19

After refusing to pay ransom, US-based auto parts distributor has sensitive data leaked by cybercriminals

MAS revises cyber risk guidelines

18 January 2021

What you must know about 'third parties' under GDPR and CCPA

Vendor Risk Monitoring

CYBERSECURITY RISK

- Application Security
- Attack Surface
- Brand Monitoring
- CDN Security
- Credential Mgmt.
- DDoS Resiliency
- Digital Footprint
- DNS Health
- Email Security
- Fraudulent Apps
- Fraudulent Domains
- Hacktivist Shares
- Information Disclosure
- IP Reputation
- Network Security
- Patch Management
- Social Network
- SSL/TLS Strength
- Web Ranking
- Website Security

FINANCIAL RISK

- Revenue Risk
- Profitability Risk
- Credit Rating Risk
- Cash Flow Risk
- Liquidity Risk
- Efficiency
- Bankruptcy Risk
- Negative Incidents

Vendor Risk Monitoring – Beyond Cyber & Financial....

CYBERSECURITY RISK

FINANCIAL RISK

ESG RISK

Environmental
- Climate-related disclosures
- Water
- Biodiversity
- Carbon Footprint

Societal
- Diversity and Inclusion
- Health and Safety
- CSR
- Human Rights

Governance
- Ownership
- Shareholder rights
- Sanctions
- Ethics

OPERATIONS RISK
- Organizational Changes
- Disruptions
- Customer Churn
- People
- Negative Incidents

COMPLIANCE RISK
- Regulation - BFSI
- Regulation - Healthcare
- Regulation - Applicable Across Industries
- Compliance
- Legal Actions
- Negative Incidents

Nth PARTY RISK
- Finance
- Operations
- Compliance
- Cyber
- ESG
- Location

LOCATION RISK
- Geo-Political
- Legal
- Business
- Financial
- Macro-economic
- Scalability
- Infrastructure
- Quality of Life

DVV solutions

SUPPLY WISDOM®

Awareness Vectors

RISK INTELLIGENCE VECTORS

INTERNAL RISK NOTIFICATIONS

1. Internal incidents and threshold violations
2. Audit findings and controls violations

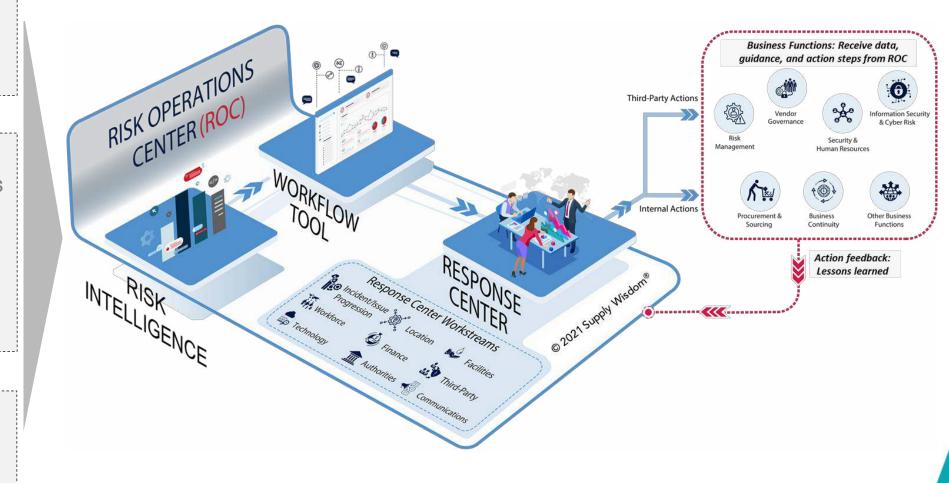### EXTERNAL RISK FEEDS

THIRD-PARTY RISKS

1. Financial
2. Cybersecurity
3. ESG
4. Compliance
5. Operations
6. Nth Party

LOCATION RISKS

1. Geo-Political
2. Legal
3. Financial
4. Scalability
5. Macro-Economic
6. Infrastructure
7. Business
8. Quality of Life

PREDICTIVE ANALYTICS

Preditive risk intelligence based on lookbacks, category and sub-category analysis, and historical incident data
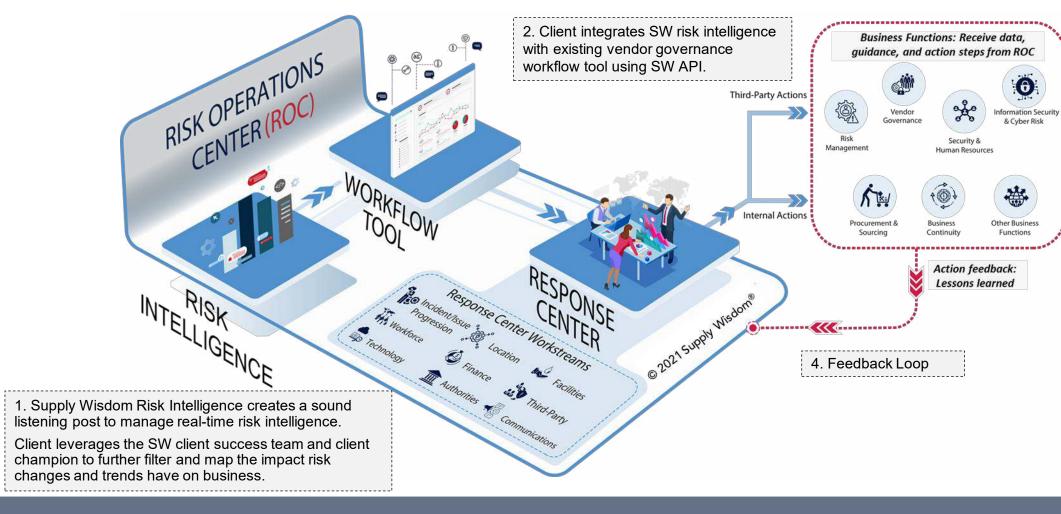
Risk Operations Centre (ROC)

Enhanced Risk Operations with Continuous Risk Intelligence

2. Client integrates SW risk intelligence with existing vendor governance workflow tool using SW API.

Business Functions: Receive data, guidance, and action steps from ROC

- Vendor Governance
- Information Security & Cyber Risk
- Risk Management
- Security & Human Resources
- Procurement & Sourcing
- Business Continuity
- Other Business Functions

3. Risk decision makers ingest intelligence provided by analysts and apply mitigation strategies to bring risk exposure back to risk appetite.

They leverage SW client success team for managing response activities and actions taken.

Third-Party Actions

Internal Actions

Action feedback: Lessons learned

4. Feedback Loop

1. Supply Wisdom Risk Intelligence creates a sound listening post to manage real-time risk intelligence.

Client leverages the SW client success team and client champion to further filter and map the impact risk changes and trends have on business.

© 2021 Supply Wisdom®

Q & A

Key Takeaways

✓ **Cyber & Financial risk optics are not enough**

✓ **Broader GRC requirements will have real impact**

  • Operational Resilience, ESG

✓ **Single pane of glass view required**

✓ **Structured way to "Measure, Manage & Respond"**

✓ **Leverage Community & Industry Resources**

  • Shared Assessments Program & Tooling

RECOMMENDED RESOURCES

Return to the Workplace…
What if They Say No?

CRO WISDOM
Supported by
Supply Wisdom

CRO Wisdom
Sharing the Wisdom of Risk Leaders

DVV **solutions**

To discuss your third party risk management challenges and how to generate scale and results in your TPRM program:

sobrien@dvvs.co.uk

+44 (0)161 476 8701
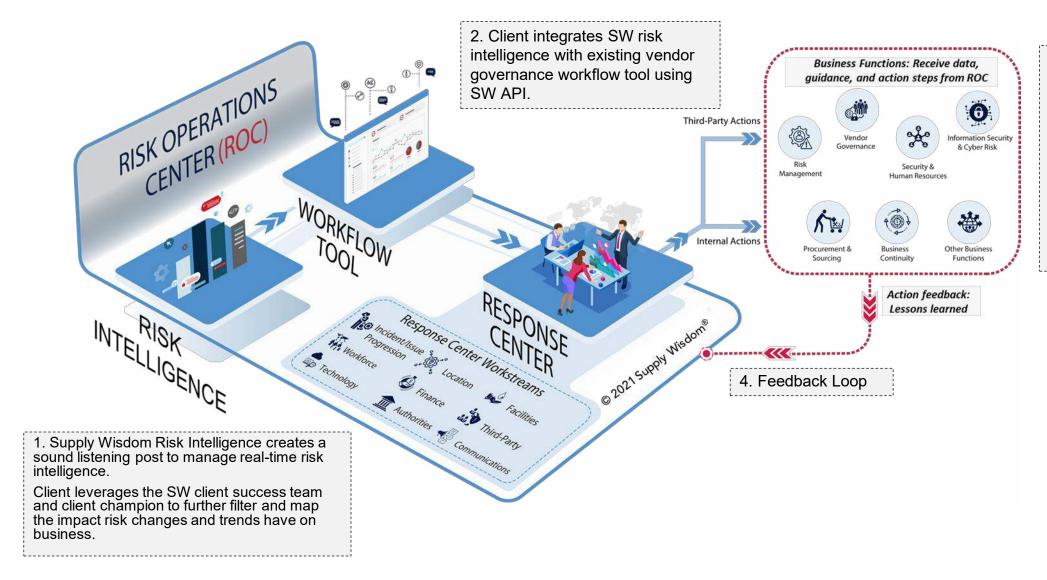+44 (0)7973 295 997

dvv-solutions

dvvs.co.uk

SUPPLY WISDOM RISK OPERATIONS CENTER (ROC)
USE CASE: ENHANCED RISK OPERATIONS WITH CONTINUOUS RISK INTELLIGENCE

2. Client integrates SW risk intelligence with existing vendor governance workflow tool using SW API.
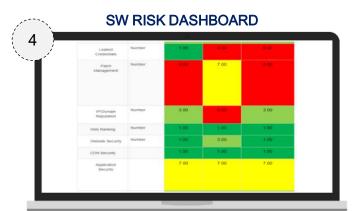
3. Risk decision makers ingest intelligence provided by analysts and apply mitigation strategies to bring risk exposure back to risk appetite.

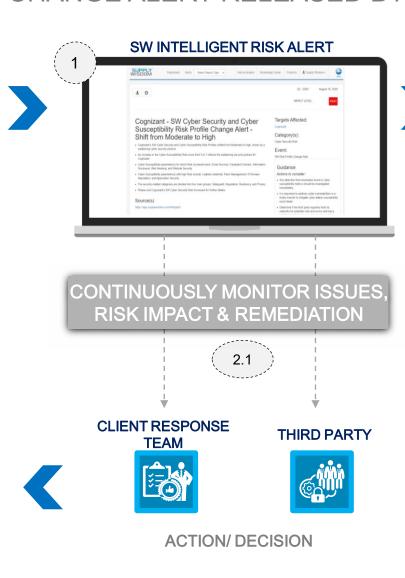They leverage SW client success team for managing response activities and actions taken.

Business Functions: Receive data, guidance, and action steps from ROC

Risk Management
Vendor Governance
Security & Human Resources
Information Security & Cyber Risk
Procurement & Sourcing
Business Continuity
Other Business Functions

Third-Party Actions

Internal Actions

Action feedback: Lessons learned

4. Feedback Loop

© 2021 Supply Wisdom®

Response Center Workstreams

Incident/Issue Progression
Workforce
Technology
Location
Finance
Facilities
Authorities
Third-Party
Communications

1. Supply Wisdom Risk Intelligence creates a sound listening post to manage real-time risk intelligence.

Client leverages the SW client success team and client champion to further filter and map the impact risk changes and trends have on business.

AUTOMATED RISK INTELLIGENCE: VALIDATE VENDOR MITIGATION
USE CASE: RISK PROFILE CHANGE ALERT RELEASED BY SUPPLY WISDOM

SW INTELLIGENT RISK ALERT

1

- Intelligent Risk Alert notifies client users on deterioration of 3rd party cyber susceptibility controls.
- Pre-set thresholds push notification to central workflow tool through SW API, and perform automated risk actions like notifying CISO office, raising a ticket with the said 3rd party, etc.

5
- Intelligent Risk Alerts notify users if risk remains unchanged or escalates

CLIENT USERS

2

WORKFLOW TOOL

CONTINUOUSLY MONITOR ISSUES, RISK IMPACT & REMEDIATION

SW RISK DASHBOARD

4

Leaked Credentials	Number	1.00	8.00	9.00
Patch Management	Number	3.00	7.00	8.00
IP/Domain Reputation	Number	3.00	8.00	3.00
Web Ranking	Number	1.00	1.00	1.00
Website Security	Number	1.00	3.00	1.00
CDN Security	Number	1.00	1.00	1.00
Application Security		7.00	7.00	7.00

2.1

CLIENT RESPONSE TEAM

THIRD PARTY

- SW continues to monitor relevant risk categories and risk metrics to identify impact of 3rd party action on external susceptibility risk

ACTION/ DECISION

- Workflow tool triggers additional risk actions based on pre-set rules – like triggering an assessment, escalating to relevant stakeholders, etc.
- Client response team is alerted if human intervention is required

3

AUTOMATED RISK INTELLIGENCE: VALIDATE VENDOR MITIGATION
USE CASE: CLOSURE AND RE-OPENING OF 3RD PARTY OFFICES DUE TO PANDEMIC

5 ▪ Intelligent Risk Alerts notify users if risk remains unchanged or escalates
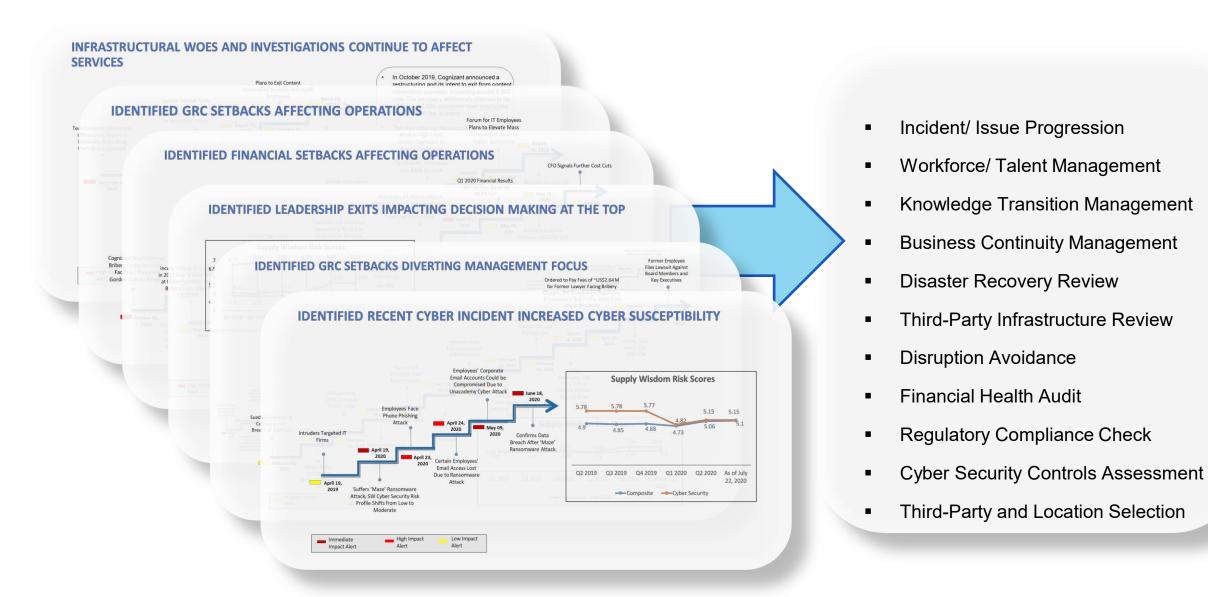
1 SW INTELLIGENT RISK ALERT

▪ Intelligent Risk Alert notifies client users on possibility of 3rd party offices being shut due to COVID-19 restrictions in India
▪ Pre-set thresholds push notification to central workflow tool through SW API, and perform automated risk actions like notifying BCM group, invoking BCP/DR plans of 3rd party, etc.

4 SW RISK DASHBOARD

CONTINUOUSLY MONITOR ISSUES, RISK IMPACT & REMEDIATION

CLIENT USERS

WORKFLOW TOOL

2

2.1

SW continues to monitor relevant changes and updates to situation, and performs required actions

CLIENT RESPONSE TEAM

THIRD PARTY

ACTION/ DECISION

▪ Workflow tool triggers additional risk actions based on pre-set rules – like triggering work from alternate site/ vendor, escalating to relevant stakeholders, etc.
▪ Client response team is alerted if human intervention is required

3

SUPPLY WISDOM: CASE STUDY
CASCADING RISKS IDENTIFIED AND PROACTIVE ACTION TAKEN

- Incident/ Issue Progression
- Workforce/ Talent Management
- Knowledge Transition Management
- Business Continuity Management
- Disaster Recovery Review
- Third-Party Infrastructure Review
- Disruption Avoidance
- Financial Health Audit
- Regulatory Compliance Check
- Cyber Security Controls Assessment
- Third-Party and Location Selection

SUPPLY WISDOM - AUTOMATED ACTION
ACHIEVE CONTINUOUS COMPLIANCE AND RESILIENCY

Reporting
- Comprehensive report of incident
- Different versions of the AAR Report are developed according to the audience. For example, the Management report may be different from any regulatory reporting

Notification
- Single risk trigger breach-direct incident that has crossed an acceptable threshold and requires immediate action
- Multi-Indicator trigger breach-combination of multiple subcategory indicators that when combined using the clients predefined parameters indicates a potential risk incident

Incident Opened
- A "case file" should be opened to initiate the tracking and incident management protocols

Validation
- All notifications must be validated before escalation or any next steps, unless the notification has been confirmed by a second source simultaneously with step one

After Action Review (AAR)
- Detailed step by step analysis of what worked and did not work

Escalation 1
- Consistent with predefined protocols, various individuals and/or functions are notified of the situation
- Consistent with predefined protocols external resources and partners are notified
- Consistent with predefined protocols Local and National agencies notified

Escalation 4
- The ROC team continues to update all appropriate persons on actions, status, including both inbound and outbound communications
- Escalates issues, rod blacks and challenges in the Recovery process
- Additional Incidents/Case Files opened as required

RISK OPERATIONS CENTER (ROC)

Interdiction
- Different from Mitigation, this is the step where actions are initiated to prevent further damage or loss. For example, an immediate, automated transfer to a back up power source due to a power grid failure.
- In some cases, there may not be a predefined action, and the people from Escalation 1 develop the action and involve additional SMEs as appropriate

Recovery
- Plans for return to normal operations
- Continuous tracking of progress
- Be prepared to track multiple related action plans or "swim lanes"

Escalation 3
- The ROC team continues to update all appropriate persons on actions, status, including both inbound and outbound communications
- Begins to distribute plans and actions to get ready for the Recovery Phase

Mitigation
- Predefined as well as Ad Hoc actions are developed, validated and implemented as appropriate

Escalation 2
- The ROC team continues to update all appropriate persons on actions, status, including both inbound and outbound communications