Risky Relationships: A Holistic View of Third-Party Risk Management

Josh Rapp, Cisco - Senior Information Security Compliance Engineer

January 11, 2023
Thank You to Our Sponsors

Platinum Sponsor

Gold Sponsors

AUDITBOARD

SOAProjects

Grant Thornton

Crowe

RGP

To the Power of Human™
Housekeeping

**Session:**
- 50 Minutes session with Q&A
- Participant audio and video are disabled
- Please use Q&A button to submit your questions for the speaker at any time
- Use chat to share your feedback or other comments if any
- Session recording will be available after this session

**CPE Eligibility:**
- Attend 50 minutes and answer at least 3 out of 4 polling questions for earning CPE
- CPE certificate will be sent to eligible participants within 2 weeks

If you are interested in speaking or volunteering, please contact us at contact@iiasj.org
Speaker Introduction

Josh Rapp
Cisco - Senior Information Security Compliance Engineer
Agenda

- Definition and Objective
- Current State
- Back to Basics
- Third Party Risk Management Lifecycle
- Investment Considerations
What Is Third-Party Risk Management?
What is Third-Party Risk Management?
“Reduce the risk of a third-party adversely impacting an organization from achieving its business objectives”
Poll #1
Current State
Resiliency
72%

Stated that the pandemic has had a negative impact on our company.

55% Most negative impact

17% Significantly negative impact
Resiliency

War in Ukraine – Supply Chain Impacts
US COMPANIES

- **450+** firms in the U.S. have tier-1 suppliers in Ukraine
- **2,100+** U.S.-based firms have at least one direct supplier in Russia
- **15,000+** firms in the U.S. have tier-2 suppliers based in Ukraine
- **65,000+** firms having connections to Russian suppliers at tier-2
- **190,000+** firms in the U.S. have Russian or Ukrainian suppliers at tier-3

SOURCE: INTEROS | www.interos.ai | ©2022
Resiliency

Environmental
- Renewable fuels
- Greenhouse gas (GHG) emissions
- Energy efficiency
- Climate risk
- Water management
- Recycling processes
- Emergency preparedness

Social
- Health and safety
- Working conditions
- Employee benefits
- Diversity and inclusion
- Human rights
- Impact on local communities

Governance
- Ethical standards
- Board diversity and governance
- Stakeholder engagement
- Shareholder rights
- Pay for performance
A data breach in the US costs over twice the global average.

For the 12th year in a row, the United States holds the title for the highest cost of a data breach, USD 5.09 million more than the global average.

https://www.ibm.com/reports/data-breach
Poll #2
Back To Basics

Centralized Inventory
- Inventory Tracking
- Contact / Document Management
- Access Management

Risk-Based Decision Making
- Tiered Prioritization
- Tailored Due Diligence
- Risk Intelligence

Third-Party Governance
- Central Reporting
- Enforcement
- Process Integration

Automation / Data Analytics
- Tech Stack Inventory
- Continuous Monitoring
- Real-Time Alerts & Reporting
The Third-Party Lifecycle
Poll #3
Third-Party Risk Management Lifecycle

Selection & Assessment
- Recommended Third-Parties
- Business Evaluation
- Tiering / Criticality
- Due Diligence

Contracting & Onboarding
- Contract Negotiations
- Contract Signing
- Access Management

Offboarding & Renewal
- SLA Performance
- Accepted Risk Review
- User Access Review
- Data Privacy Evaluation

Continuous Monitoring & Response
- SLA Tracking
- Key Risk Indicators
- Continuous Assessment
- Incident Response
## Tiering

<table>
<thead>
<tr>
<th>Tier</th>
<th>Description</th>
<th>Business Critical</th>
<th>Sensitive Data Access</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Critical to business operations and have access to sensitive data | ✔️ ✔️ ✔️           |                       | • Core service / product provider  
• Alternative third-parties not available in event of failure  
• Sensitive data is stored, processed, or transmitted |
| 2    | Not critical to business operations, but have access to sensitive data | ✔️ ✔️ ✔️           |                       | • Component service / product provider  
• Alternative third-parties available in event of failure  
• Sensitive data is accessible |
| 3    | Not critical to business operations and do not have access to sensitive data | ✔️ ✔️ ✔️           |                       | • Limited service / product provider  
• Alternative third-parties available in event of failure  
• Sensitive data is not accessible |
Due Diligence

**Risk Factor Considerations**
- Resiliency
- Solvency
- Security Controls
- Regulatory Compliance
- AML / KYC / ABC
- Corporate Social Responsibility
- Health and Safety

**Third-Party Provided**
- Completed Assessments
- Penetration Test Reports
- Contract Review

**Public Sources**
- Public Watchlists
- Data Breach Sites
- Review Sites
- Social Media & News

**Private Sources**
- Credit Reporting Agencies
- Legal Action Sites
- Threat Feeds

**Technology Integrations**
- Risk Intelligence Feeds
- Third-Party Rating Services
- Assessment Exchanges

**Public Sources**
- Public Watchlists
- Data Breach Sites
- Review Sites
- Social Media & News

**Risk Factor Considerations**
- Resiliency
- Solvency
- Security Controls
- Regulatory Compliance
- AML / KYC / ABC
- Corporate Social Responsibility
- Health and Safety

**Third-Party Provided**
- Completed Assessments
- Penetration Test Reports
- Contract Review

**Technology Integrations**
- Risk Intelligence Feeds
- Third-Party Rating Services
- Assessment Exchanges

**Private Sources**
- Credit Reporting Agencies
- Legal Action Sites
- Threat Feeds

**Public Sources**
- Public Watchlists
- Data Breach Sites
- Review Sites
- Social Media & News
Third-Party Risk Management Lifecycle

**Selection & Assessment**
- Recommended Third-Parties
- Business Evaluation
- Tiering / Criticality
- Due Diligence

**Contracting & Onboarding**
- Contract Negotiations
- Contract Signing
- Access Management

**Offboarding & Renewal**
- SLA Performance
- Accepted Risk Review
- User Access Review
- Data Privacy Evaluation

**Continuous Monitoring & Response**
- SLA Tracking
- Key Risk Indicators
- Continuous Assessment
- Incident Response
Investment Considerations
The biggest barrier to a more integrated and holistic approach to third-party management, is that the related systems do not seamlessly integrate with each other.

Deloitte Third Party Risk Management Survey 2022
Investment Considerations

- Integrate and Centralize
- Use What You Have
- Test, Test, Test
- $$$ Talks
Poll #4
Q&A

https://www.linkedin.com/in/joshrapp/
Resource List

Deloitte Third Party Risk Management Survey 2022
Prevalent Third Party Risk Management Study 2022
Venminder State of Third Party Risk Management
IBM Data Breach Report 2022
McKinsey Supply Chains to Build Resilience Manage Proactively
EY How COVID-19 impacted supply chains and what comes next
ProcessUnity ESG Reporting Mandates for TPRM
Ponemon Report State - Third Party Access Risk
Prevalent Third Party Risk Intelligence
Interos Ukraine Crisis Resource Center
Thank You!

Next Webinar:
Second Line of Duty Roles & Responsibilities
February 8, 2023