ECHELON RISK + CYBER

Third Party Risk Roundup

GETTING A 360-DEGREE VIEW OF VENDOR RISK

The scope of involvement for the third party risk management profession is rapidly expanding beyond assessments and cyber analysis, and most TPRM programs are not equipped and prepared to adapt to these changes. As organizations expand the scope of risk coverage, TPRM professionals must be prepared to rise to the challenge and know how to acquire and analyze various forms of data. In this session, we will discuss the importance of "risk intelligence" and discuss strategies to assess the various risk landscapes in order to provide holistic risk intelligence to their stakeholders.

April 26, 2023

Introducing… Echelon Risk + Cyber's Tom Garrubba

Tom.garrubba@echeloncyber.com

Tom Garrubba, Director of TPRM Services at Echelon Risk and Cyber, is an internationally recognized thought leader, lecturer, commentator and blogger on business, cyber and privacy risk. He is an instructor for the Shared Assessments' Certified Third Party Risk Professional (CTPRP) and Assessor (CTPRA) programs. With his more than 20 years' experience in cyber, privacy, audit and compliance, and consulting, he's provided thought leadership for countless industry outlets including Forbes, Bloomberg, SC Magazine, The Huffington Post, Corporate Compliance Insights, Risk.net, CIO Magazine, The Center for Financial Professionals (CeFPro), Government Health IT, Future of Outsourcing Magazine, and ISACA, He's authored the chapter on Third Party Risk for the Risk.net book "Cyber Risk" and has been featured on numerous podcasts including Business Security Weekly and the Virtual CISO Podcast. He is host of "TPRM Tidbits", weekly LinkedIn podcast focusing on current TPRM topics, and is in an instructor for such third party risk management certifications as the CTPRP and the CTPRA.

Previously, Tom was a Vice President at Shared Assessments where he was both a SME and their CISO. He was also a Senior Privacy Manager at a Fortune 10 US-based Healthcare company where he implemented and managed a world-class third party risk program. He is a member of the Forbes Technology Council and the InfraGard – Pittsburgh chapter. He also serves on the Board of Directors for the Pennsylvania-based non-profit, Pathways and serves as a 1st Lieutenant in the US Civil Air Patrol,

Education

- MS - Information Technology Management, Robert Morris University
- BSBA - Finance, Robert Morris University

Certifications

- CISA – Certified Information Systems Auditor
- CRISC – Certified in Risk & Information Systems Controls
- CIPT – Certified Information Privacy Technologist
- CTPRP – Certified Third-Party Risk Professional
- CTPRA – Certified Third-Party Risk Assessor

AGENDA

1. What Generation is Your Program?

2. Identify and build relationships to get your program there

3. Identify tools to assist your program's 360-degree scope of view

4. Design your program based on your current/existing abilities

5. Share the fluidity of you program with business partners

WHAT GENERATION IS YOUR PROGRAM?

There are **FIVE** TPRM Generations

1st Generation = Standardized Questionnaire

- ✓ SIG, homegrown questionnaire

2nd Generation = Standardized Framework

- ✓ Industry, Location, Data

3rd Generation = Technologies, Ratings

- ✓ GRC's, Cyber CM Tools

WHAT GENERATION IS YOUR PROGRAM?

TPRM Generations

4th Generation = Program convergence, Non-Cyber Risk Monitoring, Professional Certifications

✓ TPRM intersects with S&P, Legal, Financial, Social Media; Industry recognized certs such

5th Generation = Program Cohesion & VIC's

✓ TRPM is PART of Procurement & Sourcing; Center's of Excellence, Vendor Intelligence Centers (VIC)

WHAT GENERATION IS YOUR PROGRAM?

Vendor Intelligence Center (VIC)

- Acquire – data from accurate sources
- Analyze – data based on defined attributes
- Assess – the risk AND vendors
- Advise – the business unit via customized reports based on their tolerance

- ***Note**: Often times, organizations that provide this service do not provide the <u>assessment</u> of vendors, however, "next gen" will make TPRM programs a full "One-stop shop"*

2) IDENTIFY & BUILD RELATIONSHIPS

❑ Identify all of the significant internal/external organizations that your program may/will rely on for success. Examples of these organizations include:

- IT and IT Security (cyber monitoring)
- Privacy (data mapping, geolocational, legal)
- Sourcing & Procurement (business, financial, social, legal)
- Human Resources (background checks, drug screening)
- Business Continuity (testing , BIA analysis)
- Facilities Management (physical access)
- Legal (legal and business monitoring)
- Compliance (laws, standards, and aligned frameworks and guidance)

3) IDENTIFY TOOLS TO ASSIST YOUR PROGRAM

- ❑ There are numerous tools to assist you in your efforts. Identify and incorporate those tools that can provide immediate assistance and results to business partners. Types of tools for consideration include:
  - TPRM platforms
  - Data mapping
  - Cyber monitoring tools (cyber ratings, TPR security risk, DLP, etc.)
  - Specialized monitoring tools (ESG, Finance, Legal, etc.)
  - Risk assessment tools (e.g., SIG, CAIQ, ISO, NIST/CISA, PCI)
- ❑ If other organizations are already running these tools, see if you can:
  - Receive timely reports
  - Provide input as to monitoring prospective, new, or existing vendors
  - Provide scoping for the monitoring tools (don't suffer from "information overload")
- ❑ Establish practices to fully utilize the tools to support the stakeholders

4) DESIGN YOUR PROGRAM BASED ON YOUR CURRENT/EXISTING ABILITIES

□ Build your program’s needs off of your current posture such as:

- Staffing/resources
- Budget
- Number of assessments
  - Total to be performed
  - Total critical vendors
- Business line KPI’s and KRI’s

□ BUT… consider the risk monitoring needs of your business stakeholders

- Can you take on their monitoring needs?
  - If not, what do you need to help them?

5) SHARE THE FLUIDITY OF YOUR PROGRAM

❑ Modifications to any TPRM program are fluid of the significant internal/external organizations that your program may/will rely on for success.

❑ Meet regularly with your strategic partners (i.e., first and second business units) to identify and understand their vendor/supplier needs:

  ❑ What more can we do to assist them?

  ❑ If they are currently using monitoring tools, are they calibrated correctly to monitor their risks?

  ❑ Is there a need for better tools? Can you assist them in their hunt?

❑ Document the changes you're making to the program along with evidence of partner buy-in.

CASE STUDIES

- ❑Fortune 500 Retail company – Geolocational/political monitoring
- ❑Fortune 500 Bank Company – ESG monitoring
- ❑Fortune 100 Financial Company – Cyber monitoring prior to onboarding
- ❑Fortune 100 Healthcare Company – Cyber monitoring for existing vendors

IN SUMMARY

1. Identify what Generation your program is and where you’d like it to go
2. Identify and build relationships that will take your program there
3. Identify tools and practices to assist your program’s 360-degree scope of view
4. Design your program based on your current abilities but consider the needs of your stakeholders
5. Design your program to be fluid and share the news of that fluidity within the organization

Tom Garrubba

Director of TPRM Services

CISA, CRISC, CIPT, CTPRP, CTPRA

e. tom.garrubba@echeloncyber.com

p. +1 (412) 720-4248

w. https://echeloncyber.com/

ECHELON
RISK +
CYBER

ECHELONCYBER.COM