THIRD PARTY
RISK ASSOCIATION

Q3 Healthcare & Health Insurance Special Interest Call

For your awareness, this call is being recorded

THIRD PARTY RISK ASSOCIATION

AGENDA

- Welcome & Opening Remarks
- Special Interest Calls Defined
- Discussion:
  - Fourth/Fifth Party Risk Management – Visibility into risks.
  - How to identify common suppliers for all (Choke Points)
  - Medical Devices – Relationship between med device manufacturers and resellers
  - Accurately Rating Vendors
  - Business Associate Agreements
  - Data Exchange with a Partner
  - Cloud Platform Risk Management
  - Supply Chain Vendor Risk Management
- Closing Remarks

WELCOME - Introductions

Call Facilitator - OPEN
Facilitator Back-up – OPEN

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks

- **Fall Virtual Conference** – "Evolving Past Point-In-Time Assessments"
  - Wednesday, August 11th from 9 AM to 5 PM Central.
  - FREE for Members and Non-Members
  - 7 Hours of CPE
  - Speakers will present on a variety of topics that address emerging risks, continuous monitoring, critical evidence to obtain throughout the year, incorporating Artificial Intelligence (AI) into the assessment process, and innovative Third Party Risk Management (TPRM) techniques that will bring assessments to the next level.
  - For registering, you are entered into a raffle for a $100 Amazon Gift Card. If you opt-in to providing our speakers with your information, you are entered into an additional raffle for speaker gifts.
  - Please visit our conference site under "Events" or go to https://www.tprassociation.org/2021-virtual-conference.

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks

- 7/15 @ 1 PM CST - Finance & Insurance Special Interest Call - Guest Speaker - ISS Corporation on ESG Scoring
- 7/20 @ 10 AM CST - Manufacturing Special Interest Call
- 7/20 @ 1 PM CST - Technology Special Interest Call
- 7/22 @ 10 AM CST - TPRA Focus Group: Assist TPRA with building out our TPRM 101 Guidebook.
- 8/12 @ 10 AM CST – TPRA Practitioner Meeting – Panel Discussion on Continuous Monitoring

TPRA | THIRD PARTY RISK ASSOCIATION

Special Interest Calls Defined

- This quarterly call is for those who work within the **Healthcare & Health Insurance** industry (hospital system, health insurance, ancillary products, etc.)
- Topics for this call will be geared towards successes and pain points for third party risk management programs in organizations within this industry, as well as external impacts to this industry that affect third party risk management programs (such as HIPAA and HITECH).
- Agendas for each call are set my the members of the Special Interest group.
- The group is able to bring in subject matter experts to discuss a specific topic, so long as member information is not shared with the presenter. The presenter may share his/her information with the group and a member of the group may choose to reach out to the presenter for additional information.
- If the members so choose, a directory will be created and shared with members of a Special Interest group.
- Members may also choose to start a forum post specific to the industry.
- Special Interest groups may also choose to meet during the in-person conference.

TPRA | THIRD PARTY RISK ASSOCIATION

Discussion - Risk remediation

- How are you working with your vendors on remediation of findings and are they working with you?
- How are you tracking remediation?
- How are you doing this at scale?

THIRD PARTY RISK ASSOCIATION

Risk Rating	GRC	TPRM Platform	Onsite Assessment	Security Sources	Questionnaires
BitSight	Archer	Censinet	TruSight	Several	Shared Assessments
RiskRecon	ServiceNow	GraphiteConnect			
SecurityScorecard	ProcessUnity	In-House Build			
RapidRatings	Navex	Microsoft Teams			
NormShield	Unidentified Tool	OneTrust			
UpGuard	Lockpath	CyberGRX			
	Modulo/SAI Global 360	WolfPAC			

Discussion – TPRM Tools

- What tools organizations are using and pros/cons with each.
  - Archer, ServiceNow
  - Questionnaires – Home grown
  - Workday – Questionnaires, workflow, and capturing an overall vendor score

TPRA | THIRD PARTY RISK ASSOCIATION

Discussion - Cloud Platform Risk Management

- August 2020 Practitioner Meeting Playback on Cloud Security Made Easy
- Deployment models, service models, and essential characteristics
- What developers use in the cloud
- Standard & Enhanced Controls
- Control Objectives:
  - Governance, Risk, Compliance
  - Data Protection and Key Management
  - Identity and Access Management
  - Application and API Security
  - Threat and Vulnerability Management
  - Infrastructure Security
  - Virtualization Security
  - Data Center Security
- Cloud Security Alliance (CSA) – CAIQ (questionnaire)

TPRA | THIRD PARTY RISK ASSOCIATION

Discussion - Supply Chain Vendor Risk Management

- Vendor dependency
- Contract Enhancements (May 2020 Call with Nyemaster Law Firm)
  - Ordering Process
  - Delivery Process
  - Wind-down and Termination Assistance Services
  - DR/BC
  - Self-Help and Step in Rights
  - Termination or Suspension Rights
- In IRQ, asking questions around dependency on vendor and if it would be easy to switch.

TPRA | THIRD PARTY RISK ASSOCIATION

Discussion – Incident Management and Breach Response

- Engage Cybersecurity Team and Legal
- Get the Facts
  - What happened, When, What data was impacted
- Does your state have a breach notification statute?
- Enhance Contract Clauses (May 2020 Call w/ Nyemaster Law Firm)
  - Incident and Breach notification and timing
  - Investigation Rights
  - Audit Rights
- Notification of Impacted Individuals – Description, date of incident, type of information exposed, contact information for consumer reporting, advice to report suspected incidents
- Insurance
- Increase Due Diligence
  - Ask about Secure Development practices
  - Test Third Party Software
  - Ensure vendors are penetration testing and performing vulnerability management

TPRA | THIRD PARTY RISK ASSOCIATION

Topics for Next Meeting:

- Questionnaires (SIG) – Any specific healthcare industry questionnaires

TPRA | THIRD PARTY RISK ASSOCIATION

Closing Remarks

Next meeting is August 12th @ 10 AM Central.