Your Third Parties know who you are, BUT…
Do you know who they are?

Sandhya Mohan-Pillai (Director, Mobius Consulting, CGEIT, CISA)
Lee Bristow (CTO, Phinity Risk Solutions)
Learning Objectives

- What is a Third Party?
- Why are Third parties important?
- Understanding your third parties and type of relationship
- Overview of risks related to Third Parties
- Some approaches to better manage your Third party relationship
Why do they know who you are?

You

Your Third Party / Vendor / Service Provider

Know Your Customer
Why don’t you know them?

Your Office / Organisation

Outsourced call centre

Strategic Supplier

Consultant

Service Provider

Company in Group

Advisory Services

Law firm

Advisory

Outsources security services

Third Parties

VectorStock.com/2514082
History of Third Party Risk Management (TPRM)

- Still a low key topic
- Minimal CIO interest / awareness

- Evolution of regulation (Financial industry)
  - TPRM stopped being an afterthought

- Occurrence of the biggest Data Breaches

- One of the top security priorities for CISOs and Risk Departments.

- Transformation of TPRM

- Third party ecosystem is more susceptible than ever before.

- Not common
- Lack of TPRM practices

- Urgent need for TPRM
- TPRM models and programmes incorporated into business

2011
2012
2013
2014
2015
2016
2017
2018
2019
Why do you need to know them?
The Age of Change

Traditional methods of business

Mostly internal within a controlled environment

The new way of doing business

Business happens everywhere – multiple people have access to information and assets within various locations globally
Ongoing Industry Trends

- Explosive growth in outsourcing including use of Cloud service providers
- Bad Guys are targeting Third Parties
- Regulatory pressure from every angle – Regardless of industry
- Partnerships demanding good practices
- Insufficient resources
- Outdated models
Impacted Industries

Regulatory Impacts:
- SARB / FSB
- Anti-bribery and corruption
- Market Conduct
- HIPPA
- GDPR / POPIA
- Other?
What is a “Third Party”

A third party (TP) can be defined as any natural or juristic person that fulfills a service or part of a service for or on behalf of an organisation.

Such a third party may have access to the organisation’s information that may include public, personal, company confidential or special information.

The TP may reside on-site or process information remotely.
Quick Poll

Show of Hands

- Do you know who your third parties are?
- Do you know what they are doing for you?
- Do you know what risks they pose?
- Do you know what access they have?
- Do you understand how they are protecting your information?

How often are you checking/monitoring the above?
Third Party Relationships
Third Party Stranger, Danger or Strategic Partner?

• More organisations are seeking to establish partnerships
  • Longer term relationships,
  • Sharing of information,
  • Co-operation in planning

• Benefits:
  • Improved operations: higher quality, increased delivery speed and reliability, lower inventories, lower costs, higher profits.
  • Third parties can help in identifying problems and offer suggestions
  • Improved leverage model – you focus on what you are good at and your third parties focus on what they are good at
Where does it all go wrong?

• How many of you have experienced issues from your third party (e.g. Performance, SLA deviations, non-compliance?)
• How many of you have had actual incident/data breach from your third party?
Yes our premises are secure!

We have 24 hour offsite monitoring.
What can go wrong with your Third parties?

- Misuse of Access
- Data breaches
- Fraud
- Data Theft
- Lack of Compliance
Most organizations are adopting a cloud first strategy however there are some risks to consider:

- Are you aware of how the cloud vendor processes your data?
- Is the cloud vendor outsourcing to another cloud vendor?
- Is your contract sufficient to protect your data should the cloud vendor be acquired by another vendor?
- Do they have the correct controls in place to protect your data?
Manage the Risks

Overall

- Less is more
  Integrate services where possible to build strategic relationships

- Share knowledge with your TP’s (e.g. your awareness campaigns; your blueprints; your policies on information security / protection)

- Build a Partnership
  Trust & Transparency
Manage the Risks

People

- Clearly define **roles and responsibilities** of all stakeholders involved

**Internal Awareness**
- ensure all stakeholders understand the value of the process especially those responsible for the Third Party relationship

**External Awareness**
- ensure Third Parties understand the benefits. This could help their internal processes as well as ensure an improved relationship between the organisation and the client

Training

- Awareness

Change Management
Manage the Risks Processes

- Ensure there is accountability and ownership
- Ensure correct governance is in place (TP Strategy; TP Policy: TP Processes)
- Don’t try to tackle everything at once
- Third party Risk Assessment should not be too lengthy
- Ensure close integration with other third party management processes (e.g. sourcing and selection, contract management, etc.)
- Define key indicators. Monitor and report remediation progress of third parties
Manage the Risks
Technology

The TPRM process lends itself to automation due to:
• Volumes of third parties
• The repetitive nature of the process
• Operational efficiencies that can be built-in (eg automatic follow-ups)
• Audit trails
• Real-time reporting

- Ensure that a central repository of third party records is in place

- Make the process as seamless & efficient as possible (consider workflows, etc.)

- Tools are only as good as there users, ensure that the right people champion the adoption of technology.
Integrated Approach to Risk Management

Mature Governance

- Develop the required governance artefacts needed to support management
  - Policy development
  - Standards development

Mature Processors

- Implement the required process and controls and mature and gain adoption.
  - Process & procedure development
  - RACI development
  - KPI development
  - Reporting requirements
  - Develop standard response process

Automate (Tools)

- Adapt and improve through the gained efficiencies and knowledge.
Approach Applied

Set the standard for 3rd party risk management from the beginning

- 3rd party onboarding
- 3rd party classification
- 3rd party controls
- 3rd party Due diligence
- Contract management

Identify and Assess 3rd party risks annually

- 3rd party register
- 3rd party contacts
- 3rd party classification (annual)
- 3rd party Controls (annual)
- Reporting & review service levels

- The scale through automation & workflow
- Harmonize security, risk and due diligence through standard approach
- Collaborative and engage to develop trust
- Grow institutional knowledge
Third Party Risk Management in Action

TP identification

TP risk management

TP risk profiling

TP risk reporting

TP risk assessment
Final Thoughts

PARTNERSHIP

Opportunities increase when you help others win. A little win for a partner is a little win for you.

KEY PERSON of INFLUENCE.COM.AU
Thank You

Q&A