THIRD PARTY RISK MANAGEMENT

June 2019 – CISO ALLIANCE

3RD PARTY RISK MANAGEMENT

- WHAT? It is the process of analysing and controlling risks presented to your company, your data, your operations and your finances by parties OTHER than your own company OFTEN referred to as the extended enterprise
- HOW? It is the ongoing review, monitoring, and mitigation of risk over the entire lifecycle of the 3rd party engagement
- WHY? 41% to 63% of breaches involved third parties

TARGET BY THE NUMBERS

- 40m- Number of credit and debit numbers stolen
- 70m - Number of non-credit-card records stolen
- 46% - The percentage drop in profits after the incident
- $250m - Total estimated costs
- $90m - Amount paid by Target’s insurers (maxed out)
- 0 – Number of CIOs and CEOs who kept their jobs

WHAT RISKS DO 3RD PARTIES POSE

- Contractual Risk – Can the 3rd party delivery in line with expectations
- Reputational Risk - 3rd party is unable to meet expectations
- Financial Risk – 3rd Party ceases operations and can no longer fulfil it’s obligations
- Compliance/Legal Risk – what is the organisations’ exposure should 3rd Party compliance be questioned
- Information Security Risk - inappropriate disclosure, corruption, or destruction of your data
- Business Continuity –can the 3rd Party effectively recover and continue providing the contracted
- Geopolitical Risk – disruptions of service due to…

MASTERDEEDS OFFICE BREACH

- 60m unique IDs exposed
- Majority of South Africans were affected. Even certain deceased citizens!
- Dracore Data Sciences was identified as the source
- Data was leaked from the servers of property company Jigsaw Holdings after uploading the information to a public server

THIRD PARTY RISK MANAGEMENT

- What Does It Look Like?

CF16.1 EXTERNAL SUPPLIER MANAGEMENT PROCESS

- Identify and categorise external suppliers (group 1)
- Assign a business AND security owner
- Agree on security arrangements (group 2)
- Validate those arrangements (audit) (group 3)
  - Documentation review
  - On-site review
  - Identify inherent/residual risk
  - Agree remediation plan
  - Ongoing monitoring and/or reviews based on Tier
- Have a plan to terminate (Group 4)

BENEFITS

- data breach costs ⬇
- Reduce likelihood of costly operational failures ⬇
- Reduce likelihood of vendor bankruptcy ⬇
- Regulatory mandates may require it
- Ethical obligation
- ?

SUMMARY

- 70% of companies do not adequately do this now, yet over 90% say they will INCREASE their use of third parties.
- Given the risk exposure and costs involved, TPRM can be the single most cost-effective risk management program that a company can implement