CYBER RISK

NED Talk Book

October 2022

IDEAS | PEOPLE | TRUST

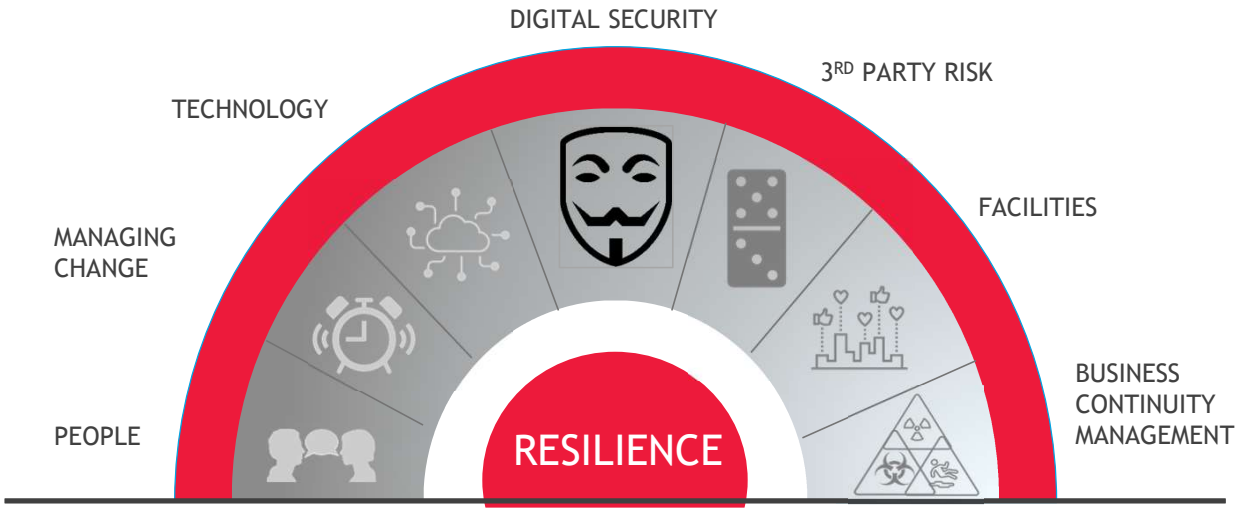
BDO

WHAT IS CYBER RESILIENCE?

"Cyber resilience refers to an entity's ability to continuously deliver business operations with limited or no degradation of services, despite Cyber attacks"

The FCA and PRA have recently defined Operational Resilience as the ability of the Financial Services sector to prevent, adapt, respond to, recover and learn from operational disruptions.

This definition extends perfectly to other sectors, especially where Cyber is a key risk. Understanding your organisation's Cyber Risk profile across the key resilience areas will enable you develop an understanding as to whether an organisation adequately manages its Cyber Risk profile.

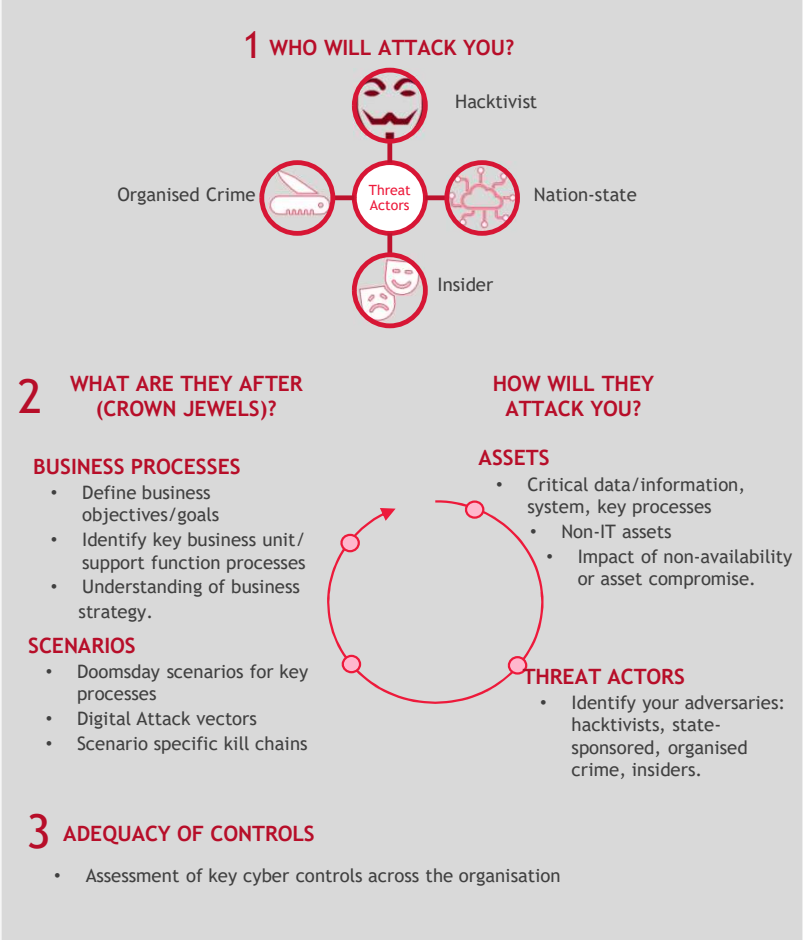


UNDERSTANDING CYBER RISK

Risk Identification

Cyber attacks come in different forms and range from basic to highly sophisticated attacks, often combining with the human element. Your organisation's ability to defend against these attacks will be a combination of IT/the business understanding its Cyber Risk profile. At a high level, this consists of three activities which should form a basis for the development of your Cyber Security Strategy and the continual updating thereof, as follows:

1. Threat Modelling – Understanding who the Threat Actors are who will target the organisation
2. Business Value Chain (Crown Jewels Assessment) – Understanding the value chain of the organisation, including key business processes, assets, scenarios for risk and likely threat actors
3. Adequacy of controls – Assessment of key cyber controls within the organisation. Recommended framework assessments are NIST or CIS 18.



NED CHEAT SHEET ON CYBER RISK

Keeping it simple

These are some of the typical artefacts that may be shared with NEDs. The list can equally be treated as a request list for NEDs seeking to understand an organisation's Cyber Resilience. Some critical questions to consider when reading or engaging are set out below.

CYBER SECURITY STRATEGY

It should not be taken for granted that an organisation will have a Cyber Security Strategy. Evaluating the one you receive will be easier with the following critical thinking front of mind:

- Does the Cyber Strategy consider the likely threat from the various threat actors and does it clearly articulate the inherent risk to the business value chain (Refer to slide 3 Crown Jewels Assessment)? Consider whether it is accurate.
- Has IT assessed the Cyber Control environment against an industry recognised framework?
- Does the *"to-be"* desired Cyber Security posture align to the risk appetite of the organisation?
- After reading the strategy are you confident that both *"as-is"* and *"to-be"* have been clearly articulated?

CYBER ASSURANCE (2ND OR 3RD LINE ASSURANCE)

Assurance over Cyber Security is quite complex and following are typical assurance activities that could be relied upon:

- **Cyber Controls Assessment** - This should be performed yearly and aligned to a controls based assessment framework (ie NIST or CIS. Maturity and self-assessment should not be considered as adequate unless it is a Year 1 activity and self-assessed as being poor.
- **Penetration Testing** – This type of test can be performed in a number of different manners. What is critical is that the testing is aligned to the high risk components of the value chain of the business. The report should clearly articulate why that particular scope was agreed and should align to a threat profile in the context of the value chain of the organisation. The time allocated for the test should be adequate to provide assurance in identifying risk. The conclusion should be easy to read and non-technical in articulating business risk
- **Crisis Simulation** - Very often organisations will focus on IT's ability to identify, contain and recover from a Cyber Attack. While this is critically important, equally a test should be performed to assess how the Crisis Team communicates with each other and IT to manage a cyber incident. Does the organisation have the necessary skills to manage a Cyber attack? Have they contracted with 3rd parties to assist with a breach?

3RD PARTY RISK

3rd Party risk is an often neglected component of Cyber Risk. How has the organisation identified and mitigated 3rd Party risk? Consider this in the context of critical suppliers in the supply chain and IT outsource providers. The Cyber Strategy should to some extent recognise the risks associated with 3rd Parties. Can the organisation quickly identify critical 3rd Parties and is it clear when they were last assessed?

FOR MORE INFORMATION:

Jason Gottschalk
07976 597 979
jason.gottschalk@bdo.co.uk

Matthew White
07798 606 644
matthew.white@bdo.co.uk

Jo Gilbey
07800 682 7443
jo.gilbey@bdo.co.uk

www.bdo.co.uk

IDEAS | PEOPLE | TRUST

BDO