SNAPSHOT

Cyber Target Operating Model

BCS CONSULTING

Expect **Excellence**

What is a Cyber Target Operating Model?

A Cyber target operating model (TOM) is a blueprint of a firm's vision that is aligned to its operating capabilities and focused specifically on its cyber security function. An effective Cyber TOM enables a firm to effectively defend against cyber security threats and manage any residual risk. This is achieved through ensuring the right people, processes and technology are in place to identify and prepare for the cyber security threats facing the firm.

A comprehensive cyber security operating model includes:

- **Vision and Strategy** of the cyber security function.
- **Governance and MI** - ensuring accountability for cyber security up to Board-level with clear reporting lines and MI to facilitate decision making through the firm's governance structure.
- **Standards and Policies** - how the firm expects people, processes, and technology to support the management of cyber risk in adherence with cyber security regulations and standards.
- **Process and Automation** – embedding cyber standards and policies within the firm's processes, automating where possible to increase efficiency and covering the five core NIST functions: Identify, Protect, Detect, Respond and Recover.
- **Technology and Data** - embedding technology and data in line with the cyber security vision and strategy and ensuring it appropriately supports each process. Data should be integrated into dashboards to present meaningful MI to relevant stakeholders.
- **People, Organisation and Culture** - the successful recruitment and retention of skilled cyber security professionals and definition of how they will work with the wider firm via defined roles and responsibilities.
- **Sourcing and Location** to outline the required location of cyber security staff and the approach to sourcing.

Why is it important to the market?

Whilst significant progress has been made across Financial Services in recent years to protect customer data and critical services from cyber security threats, cyber-related risks remain top of most firms' operational risks. At BCS Consulting, we believe defining and implementing a comprehensive Cyber TOM will enable firms to address these cyber-related risks for the following reasons:

- **Recruitment and Retention of Cyber Security Professionals:** For firms to manage their cyber risk effectively they need well-trained cyber security professionals. Such professionals are in high demand and to attract and retain top cyber talent, firms need to ensure their Cyber TOM enables effective and efficient working practices and provides work that is both challenging and fulfilling.
- **Ever-Evolving Threat Landscape:** The cyber threat landscape is constantly evolving and a firm's cyber risk is directly linked to the cyber threats it is exposed to. From the early stages of developing a successful Cyber TOM, the threat landscape of the firm will need to be considered so that cyber risk can be reduced. The Cyber TOM should establish feedback loops so that changes in the threat landscape can be communicated and managed, e.g. first and second line of defence sharing vulnerability and incident MI.
- **Customer Service Benefits:** A firm's customers can be impacted by cyber events and a Cyber TOM aligned to the firm's principles can ensure the impact on customers is managed, providing a better customer service. For example, it can allow the firm to be as transparent as possible with customers when an incident occurs and provide support to affected parties. Additionally, if your TOM is set up properly it allows you to deliver cyber security services to customers that are easy for them to use and not too cumbersome.
- **Clearly Documented Governance and Oversight:** A fully documented Cyber TOM enables the firm to demonstrate there is clear ownership and accountability for cyber risk and robust governance structures in place to help manage it. This also helps to demonstrate this to regulators (e.g. as part of compliance with operational resilience and cyber risk regulation).

What is our view on it?

We have found that a clearly defined Cyber TOM and roadmap is fundamental to effectively managing cyber risk within an organisation. The people aspect of a Cyber TOM is the most frequently overlooked, which can reduce the effectiveness of a cyber security function by not having the right people in place to utilise processes and technology. Aligned to this, it is paramount that the Cyber TOM is aligned to the firm's wider TOM (especially the IT TOM) to ensure it works cooperatively with the rest of the firm and avoids creating siloes.

To address the above shortcomings, we believe there are two key areas you should review within your Cyber TOM:

1. People, Organisation and Culture

The Cyber TOM should enable you to hire, retain and retrain skilled staff, with roles for both the technically skilled and individuals who can communicate clearly with the business. Gone are the days where technical expertise is the only driving factor and it is worth considering the following as part of your cyber recruitment processes:

- Can you expand your available labour market by offering remote and flexible work?
- Are you tracking your peers to assess whether they are hiring for similar roles?
- Are you remaining competitive with your employment offering to ensure you can retain top talent?

Have you also considered outsourcing some of your cyber function's roles? For example, smaller firms may want to use a SOC managed service provider to avoid the high cost of running one themselves.

2. Governance and MI

It is also important that your Cyber TOM defines clear roles and responsibilities and management information flows between cyber security teams and the business. Reporting lines will vary depending on the size, structure, and nature of your firm, as well as direction from the regulators. You should consider whether your cyber function has:

- Defined roles with clear responsibilities and accountabilities (e.g. RACI);
- Aligned cyber security responsibilities to SMCR;
- Assessed potential conflicts of interest between the SMCR roles an individual is responsible for?

What BCS Consulting can provide

- Support to develop your Cyber TOM design principles and alignment with the vision and strategy of your firm.
- A full current state assessment of your Cyber TOM, which could include:
  - Reviewing the vision and strategy of your cyber function and how people, processes and technology have been defined;
  - Reviewing alignment of the Cyber TOM with the firm's wider operating model; and
  - Assessing the current cyber function's maturity against a selected framework (e.g. NIST).
- Support to define your Cyber TOM and roadmap and manage the implementation of the Cyber TOM and roadmap.
- Periodic reviews of your cyber security function to identify and implement further improvements.

Who should you speak to about it?

For more information please contact either

Ben Mason, Managing Director
Ben.Mason@bcsconsulting.com

Chantal Fifield, Consultant
Chantal.Fifield@bcsconsulting.com

Charlie Harries, Consultant
Charlie.Harries@bcsconsulting.com

SNAPSHOT