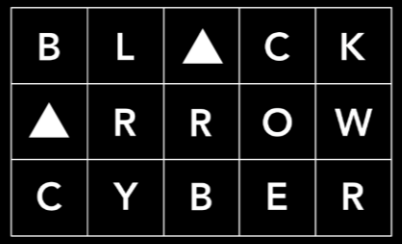
Summary notes: Cyber Security for non-IT Professionals in the Insurance Sector

March 2021



Black Arrow Cyber Consulting
About us

- Channel Islands based Cyber and Information Security consultancy.
- Former British Intelligence, UK Central Government, global Financial Services, Big-4 Consulting and the GFSC.
- Business experience across IT, Strategy, Finance, HR, Governance, Risk, Compliance and Regulation.

We help organisations and individuals to understand and manage Cyber and Information Security in plain English and with pragmatic solutions across people, operations and technology.

BLACKARROW
CYBER CONSULTING

Cyber Security for the Insurance Sector

Workshop Structure

1. Demystifying Cyber Security
2. Cyber Security for Insurance Sector
3. Cyber Hygiene: Working from Home

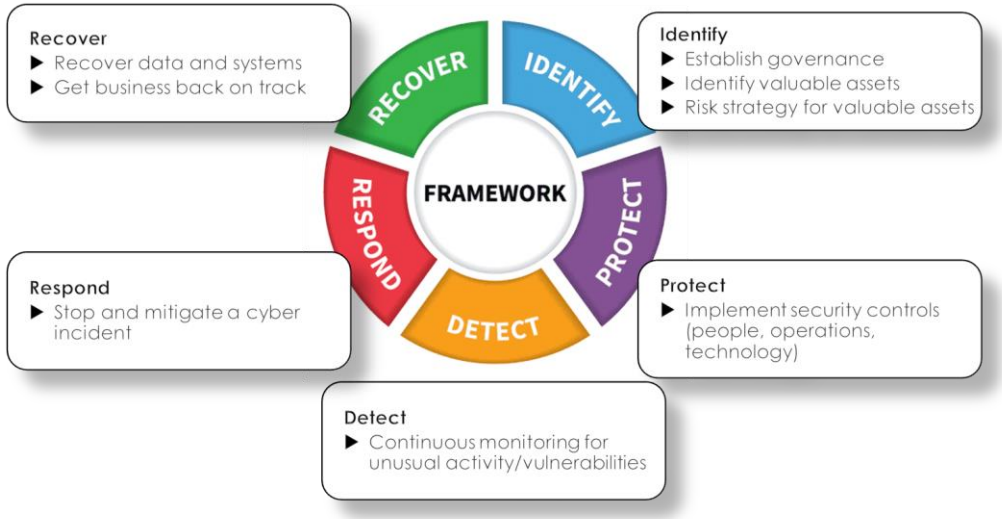
BLACKARROW
CYBER CONSULTING

1 Demystifying Cyber Security

- 'Cyber Security' and 'Information Security' are often used interchangeably but are distinct. Information Security is the wider topic of protecting information in all its forms including physical and electronic data, and documents. Cyber Security is a subset of Information Security and relates specifically to electronic data.
- Regulators and other stakeholders require Boards to take Cyber and Information Security seriously, and recent cyber incidents in the Channel Islands show the threat and impact of an incident are real.
- Cyber Security is all about balancing risks and controls to protect the confidentiality, integrity and availability (CIA) of information, known as the CIA Triad. These risks and controls can be through people, operations and technology.
- The three biggest people-enabled cyber threats that we reviewed in the webinar are email based attacks (Phishing, Spear Phishing, Whaling), other social engineering attacks (Business Email Compromise – BEC, Smishing and Vishing) and insider risk from employees that are disgruntled, in financial difficulty or who deliberately bypass the organisation's controls. Research shows that insider risk through disregarding the organisation's protective controls is especially prevalent in senior leadership.
- In the webinar, we looked at the honeypots that Black Arrow have deployed as part of our threat intelligence research. We typically see over 10 million attacks per month on local honeypots, which use the same internet connections as other businesses and individuals in Guernsey.
- We looked at the main frameworks for Cyber and Information Security: Cyber Essentials/Cyber Essentials Plus, NIST CSF and ISO 27001. They all have advantages and disadvantages, The Cyber Essentials/Cyber Essentials Plus accreditations do not fulfil the requirements of the GFSC Rules because they do not include the necessary breadth of controls such as monitoring capability to enable an organisation to know if they experience a cyber incident and to mitigate the damage.

2 Cyber Security for the Insurance Sector

- The NIST framework takes you through a circular lifecycle of the things Boards need to cover in Cyber Security. That is why it is so popular and respected, and why is it the basis of the GFSC rules.
- The five Functions of NIST, like everything related to Cyber and Information Security is a continual process, not a one-time project. Cyber risks are growing every day and businesses must take a proactive approach and continually review their capability to counter the rising tide of threats.



- The requirement for Governance, contained in the Identify Function, underpins Cyber Security. The Board members should own the Cyber Security Strategy, and monitor its implementation and ongoing suitability by regularly reviewing a dashboard of selected key metrics. This dashboard should be supplemented by robust incident reporting and threat intelligence that is interpreted for the business.
- The Board is not expected to be experts in Cyber Security but they should have a suitable understanding of the fundamentals to exercise good governance. If necessary, the Board should engage the support of trusted external experts to upskill them on Cyber Security, and it is important that the experts should be independent of the outsourced IT providers to enable objective assurance.

3 Cyber Hygiene: Working from Home

- In the first few months of COVID-19 last year, the number of phishing attacks increased by 600%. Cyber attackers exploited the fact that people behaved differently and were less security conscious when working from home. The attack surface increased exponentially and traditional IT models were less effective.
- In the webinar, we looked at what employers should do to manage their Cyber Security for employees working from home, and what employees should do to support that. This requires controls across people, operations and technology underpinned by informed and objective governance by the Board.

Assess PEOPLE controls

- Develop a 'Security First' culture, driven from the top of the organisation by leadership example.

Assess OPERATIONAL controls

- Make sure all operational processes are documented and re-evaluated to fit the reality of working from home.

Assess TECHNOLOGY controls

- Ensure that any remote access is secure, and that devices are updated with the latest secure software.
- Monitor the network for anomalous activity.

Assess GOVERNANCE and REPORTING

- Implement proactive monitoring of cyber controls across people, operations and technology by the Board.
- Ensure the Board is upskilled on the fundamentals of Cyber Security by a trusted independent specialist if necessary.

BLACKARROW
CYBER CONSULTING

blackarrowcyber.com

01481 711 988

contact@blackarrowcyber.com

---

blackarrowcyber.com/blog

twitter.com/BlackArrowCyber

LinkedIn.com/company/BlackArrowCyber