CYBER SECURITY: WHAT BOARDS NEED TO KNOW

This Factsheet has been created by Mazars Ireland exclusively for IoD Ireland members.

Even in the midst of one of the most significant events of our lifetimes, organisations need to do more to **invest in the right cyber security measures, which balances the need to run the business with the need to protect its most critical information assets.**

As cyber security budgets are squeezed during COVID-19, an organisation must take a **risk, value, and cost optimisation** approach to determining cyber security priorities and investments. It is also essential that boards include time on the agenda to discuss their cyber security approach and to continually assess and reassess their capacity to address cyber security threats. But for many organisations, it is difficult to answer the question **are we investing in adequate and effective cyber security hygiene measures to protect our most critical information and systems?**

Common challenges faced by organisations related to shortcomings in **Cyber Security Governance:**

	Challenge	Why is this an issue?
1.	**Basic or a lack of cyber security hygiene resulting in weak security.**	Organisations operating from the lowest common denominator when it comes to implementing some of the most basic security protections will fail to protect customer or company information and systems.
2.	**Organisations lead their security programs with significant investments in technology, often overlooking the human risk.**	Security capabilities are a function of people, process and technology. Cyber investments focused on technology alone, will not address the human risk, which could result in a costly compromise of customer, staff or company information and systems.
3.	**Senior management focus on achieving near to zero tolerance for cyber security risk is an unattainable outcome.**	Organisations who adopt a near to zero cyber risk appetite are just not being realistic. Developing an effective, measurable, and actionable cyber risk appetite is hard, especially given the fast-changing nature of COVID.

1.

Basic or a Lack of Cyber Security Hygiene

A basic or a lack of cyber security hygiene finding has been reported by the Information Commissioner's Office (ICO) Regulator for many of their data protection investigations. Even with the most stringent payment card industry standards that organisations must comply with relating to payment card handling, e.g. PCI-DSS. The ICO's investigation of the British Airways Data Breach found that the CVV codes on customer credit cards were left open, making them easy to cyber-attack. If your organisation is subject to cyber-attack, the Data Protection Commission (DPC) will look at whether or not your organisation left the doors open to cyber criminals, whether or not the attack was foreseeable, what kind of due diligence and steps were taken in the data security program. An organisation's Senior Management and the Board of Directors need to ask the question **'are we investing in adequate and effective cyber security hygiene measures to protect people's information'?**

MAZARS

2.

Technology Focus

Effective cyber security is less dependent on technology than you might think. While necessary, technology alone, will not address the human cyber risk, which could result in a costly compromise of customer, staff or company information and systems. In the current COVID-19 landscape, **phishing methods** are continually evolving and at an **alarming rate, according to Interpol**. Cyber criminals are targeting individuals, small, medium and large corporate and government organisations for **identity fraud and financial gain**. If they obtain access to your organisation's systems, they could also hold your personal data to ransom, blocking its access until a ransom fee is paid. Cyber criminals will also seek to acquire company intellectual property and national security information.

Organisations must prioritise within their security programs the need to train their staff to be able to recognise and know how to respond to the various types of cyber risks and threats.

3.

Near to Zero Risk Appetite

Developing the organisation's **awareness that achieving 100% protection against cyber crime is not realistic. Cyber risk should identify which processes and or systems are the most valuable** and present the most cyber threat to your organisation. You need to be clear how much risk you are willing to take with these critical processes and systems; if these processes and systems are reliant upon third party providers? If so, do third party providers have the same level of risk appetite and security measures as you? CIOs and CISOs should work with Senior Management and Board of Directors to develop an **effective and actionable cyber risk appetite and embed it into the organisation along with IT governance decision-making processes.** It is also critical that boards include time on the agenda to discuss their cyber security approach and to constantly assess and reassess their capacity to address cyber security threats.

Cyber security requires board-level attention and responsibility and is not just an IT issue. The need to ensure your organisation has in place an effective cyber risk appetite mechanism for investing in the right cyber security measures, which balances the need to run the business with the need to protect its most critical information assets has never been more important.

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT:

Sarah Hipkin
Director IT and Data Protection
SHipkin@mazars.ie

Liam McKenna,
Partner – Consulting
LMcKenna@mazars.ie