


**CYBER SECURITY – A
BUSINESS CRITICAL ISSUE**

SPACE
EXECUTIVE



January 2022

**CREATING A RISK-AWARE
CULTURE FROM THE TOP DOWN**

- 
1. The Impact of Cyber-Attacks
 2. Key Threats to be Considered When Developing a Cyber Strategy
 3. Practical Solutions to the Threats Posed by Cyber

The risk of cyber-attacks is ubiquitous, and their repercussions on the businesses they impact can be devastating.

Companies, therefore, need to ensure they are focusing resources on engendering a risk-conscious culture.

The impact of cyber-attacks on businesses include, but are not limited to:

1. Profit loss risk due to inability to operate (ransomware)
2. Operational risks in the wake of an attack
3. Business continuity management demands
4. Reputational risks
5. Regulatory costs and penalties associated with data breaches

While cyber security spending increased from \$0.9m in 2019 to \$1.9m in 2020, Gartner predicts that investment is slowing, driven by a demand from Boards to see more tangible results around data analysis and performance from the measures taken, leading to a reduction in the number of cyber-attacks occurring.



Given the high level of risk associated with cyber-attacks and their fallout, today's business leaders must take an active stance when recognising the threats cyber-attacks pose and ensuring they are well informed and educated on their impact.

"We have seen a dramatic increase in the number of companies who are looking to have cybersecurity, data privacy and data protection representatives at a Board-level.

Our clients increasingly recognise the need for specific expertise in response to the risks posed by cyber-attacks, ransomware and malware.

Leadership teams can no longer ignore the risks posed by cyber and are seeking professionals with the experience to both identify the threats and provide a practical future-proof solution."

Marek Danyluk, CEO and Managing Partner,
Space Executive

Here are some of the key threats Boards should consider when defining their cyber strategies.

Operational Risks, Employee Awareness and a Shift to Remote Working

Many companies now use technology to facilitate remote working or move to an e-version of the business. Having dispersed employees increases risks around access to systems and potentially encourages more relaxed attitudes to individual logins.

Employee awareness is becoming a critical issue in the fight against cyber-attacks. Large numbers of employees remain unaware of the cyber security training provision within their organisations.

It is vital to develop a clear cyber security strategy and ensure that employees are educated and empowered to take ownership of cyber best practice. This should be the responsibility of the whole leadership team, not just the Chief Information Officer (CIO).

1/3

Employees in the UK prioritise connection speed over secure connections.

1 in 5

Employees has fallen prey to a phishing attack.

25%

US employees use weak passwords such as 'Password' or '123456' (responsible for 30% of ransomware infections).

Legacy Systems

Specific industries such as healthcare and manufacturing have become more at risk from cyber-attacks due to reliance on legacy systems and a reluctance to switch to newer technologies due to high programme costs and time commitments.

Internet of Things

Many organisations are unaware of the risks of collecting sensitive data derived from the Internet of Things and its collation within software-as-a-service (SaaS) solutions. This lack of education around the risks presented by IoT brings a multitude of cyber security risks – particularly when you add in third parties accessing the systems – whether from an IT, product development or after-sale perspective.



Regulatory Requirements

Leadership teams need to be aware of data privacy and cyber regulatory requirements, as the financial penalties for non-compliance can be severe. Key among these is the Data Protection Act (2018) and the current General Data Protection Regulation (GDPR).

The legislation covers the fundamental principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability.

+25%

Companies are still not fully GDPR-compliant.


There are severe fines of up to £17.5m, or 4% of annual global turnover, for failing to comply with GDPR.

Over the past three years, there have been several high-profile cases, including Google (fined £43.2m), H&M (£32.1m) and British Airways (£20m).



While every organisation requires a tailored cyber strategy, here are some practical solutions that businesses can apply across all companies.

- 
1. **Build a Cyber-Conscious Culture.** Boards need to recognise the value in their data and the threats posed by cyber-attacks to ensure that support and investment in their cyber strategy is a company-wide initiative.
 - **Empower Leadership.** Ensure leadership teams are empowered to enforce group-wide adherence to their organisation's cyber strategy.
 - **Educate Employees.** Make sure all employees are aware of their company's cyber strategy and take ownership of cyber best practice.
 - **Board-Level Representation.** Cybersecurity, Privacy and Data Protection considerations require representation at a board level.
 2. **Regulatory Compliance.** Cyber strategies must comply with all regulatory requirements.
 3. **Keep Evolving.** Cyber strategies need to safeguard against today's threats and provide a future-proof solution for tomorrow.
 4. **Keep Investing.** As cyber threats evolve companies need to allocate sufficient investment in their cyber strategy to ensure it continually protects them.



A company that avoids cyber-attacks should view their investment in cyber as garnering a positive return on investment. Organisations cannot afford to underestimate the dangers of becoming complacent and reducing spending.

The growth in technology and our changing work patterns mean cyber risks are increasing. As Christopher Wray, Director at the US Federal Bureau of Investigation said:

'The scale of this is something I don't think this country has ever really seen, and it's going to get much worse.'

Should you wish to discuss this report or your hiring challenges please do not hesitate to reach out to our specialist team or visit our website www.space-exec.com.



info@space-exec.com



www.space-exec.com



London

35-41 Folgate Street
London
E1 6BX

Hong Kong

7/F K11 Atelier Victoria
Dockside, 18 Salisbury Road
Tsim Sha Tsui
Hong Kong

Singapore

168 Robinson Road,
12-01 Capital Tower
Singapore 068912