Covid-19: Cyber awareness

Ideal conditions for cyber criminals

Fraudsters are using Covid-19 as a front in phishing emails to appear to be from an authentic source, or to create a sense of urgency to click via a link.

Some are obvious to spot, others less so. For example, appeals for donations and informal funding, or finding ways to poach log-in credentials to secure sites.

Network uncertainty

As many of us are already discovering, working from home means receiving a high volume of messages on different devices/apps, and rapidly adopting new business processes without routine IT support.

It is far easier for employee errors or network security to be exposed under these circumstances.

This opens the door to cyber-attack or a malicious data breach. Ransomware attacks are likely to increase and become more damaging to a business's ability to trade.

Protecting data

Sharing personal data or confidential information outside the secure business network is inevitable as employees find ways to communicate efficiently.

For many, this is a **delayed risk**, meaning problems could emerge from data protection/GDPR concerns many months after, including the inability to effectively retrieve data.

Which sectors have specific risk?

- **Retail** – these firms will increasingly focus on e-commerce and online marketing as, for some, this is their main chance of survival. The risk shifts from physical goods and stock to intangible goods with an online presence, customer data, and ability to manage fulfilment.
- **Travel and hospitality** – similarly to retail, this sector will increasingly focus towards e-commerce. They will also be handling an exceptional amount of changes to payment instructions via email.
- **Creative industries and media** – moving activities to digital campaigns, lead generation and virtual events will involve more data processing and GDPR challenges.
- **Professional services** – challenges to longstanding methods of working/filing of data. The use of social media to generate work may give rise to new e-media risks if they accidentally breach privacy or competitor IP.
- **Key production and services** – Firms who are experiencing rapid growth to meet Covid-19 demands are having to increase capacity, and will rely on technology to scale up. These businesses should not overlook cyber risk and dependency on a network built for a smaller business.

How a Cyber policy can help:

- The policy includes cyber crime coverage, which can be further extended to cover social engineering/impersonation where no hacking has occurred.
- Cyber liability will defend you, for example, against claims where your communications have been hijacked to initiative payment fraud.
- Cyber or data breach response – emergency IT and Legal support as well as access to PR crisis management.
- Business interruption – the increase costs of working or loss of profit during any downtime, which could be made worse as routine access to servers/ hardware may be affected by Covid-19 period of lockdown.

MARKEL®