



Grant Thornton

An instinct for growth™

Mitigating risk and managing cyber crime

No organisation or industry is immune to cyber-crime.

Cybersecurity Awareness Month

As cyber-attacks dominate the headlines, regulators and stakeholders are under increasing pressure to manage cyber risk. There is more to managing digital risk than relying on technology alone, therefore businesses must adopt several non-tech measures to protect themselves.

Develop a strategy

Leaders will have to step into the shoes of cyber criminals, understand the threats these groups pose and develop proactive strategies to protect their business' interests whilst addressing their digital vulnerabilities.

Have the right structure

Internal governance, processes and people are important aspects to consider, along with ensuring the right structure is developed and adopted. Additionally, we recommend businesses undertake a structured programme to assess and validate their most valuable data assets, using a categorisation and classification process, enabling them to invest in appropriate insurance cover.

Manage trust and reputation

Businesses must understand the value they deliver to the customer, once this has crystallised, the potential impact a breach would have on the relationship can be formed, enabling effective mitigating strategies to be adopted. Businesses should consider customer

relationship managers and trust policies to correlate with the technology being used.

Educate your people

To enable its people to understand and manage risks effectively, we recommend developing shorter, more frequently distributed training videos and simulated phishing attempts, along with ensuring skilled resources are available across the business to support ongoing development.

Recruit specialised resources

Specialised cyber skills are required, therefore we recommend having access to resources who can complement cyber security technical skills with commercial acumen. This will ensure that your investment in preventive software is focused in the right areas, along with having an additional safeguard for stakeholders and the business to rely on.

Insure yourself effectively

Which email threads could a former employee leak to embarrass their former managers? What intellectual property and trade secrets would be of interest to a foreign power? And how might a cyber-criminal use your data to try to extort money from your business? These are just some of the questions you need to ask before purchasing insurance as part of your digital risk management plan.