Grant Thornton
An instinct for growth™

Cyber resilience

Effectively dealing with disruptive cyber incidents

Cyber resilience

The spectrum of cyber risks and threats is now so huge that simply implementing cyber security is insufficient. Cyber resilience, on the other hand, enables an organisation to minimise disruption and be able to continue to function in the event of a disruptive incident.

Why is business resilience increasingly important?

- In the global community, the continuous development of new technological methods to connect and share information increases the probability of a security threat.
- A survey commissioned by the UK Government in 2017[1] identified that most of the UK businesses included in the report were exposed to cyber risks. Nearly three quarters of the businesses included in the survey regarded cyber security to be a high priority although conversely, the survey highlighted that a large proportion of UK businesses do not have proper cyber resilience approaches in place.
- It is the responsibility of the board to manage an organisation's risks; this includes cyber resilience. It is important that the board is kept up to date regarding the effectiveness of the cyber security controls in place and any exposures which fall outside of the business's capacity to manage that risk.
- Poor cyber resilience diminishes any security an organisation would have if a business disruption occurred.

What happens when it all goes wrong?

- Cyber incidents are unpredictable and can strike an organisation at any time.
- Protection of an organisation's intellectual property, customer data and other critical information assets is pivotal to the growth, innovation and reputation of an organisation.
- Organisations can struggle to recover from the reputational damage caused by a disruptive event.
- Making sure a complex organisation is resilient to such threats may seem daunting. However, managing the aftermath, such as significant reputational damage, affected global operations and complex relationships, as well as commercial production, poses an arguably even more foreboding challenge.
- Robust cyber security measures are critical to protecting an organisation's reputation and its customers.

Industry guidance: business resilience in the wider industry

Our business resilience services follow the guidance contained in relevant British and international standards, including:

BS11200	BS65000	BS ISO 22301	BS ISO 22313
Crisis management:	**Organisational resilience:**	**Business continuity management systems:**	**Business continuity management systems:**
guidance to good practice	guidance	requirements	guidance

[1] Cyber Security Breaches Survey 2017 by Ipsos Mori, commissioned by the Department for Culture, Media and Sport

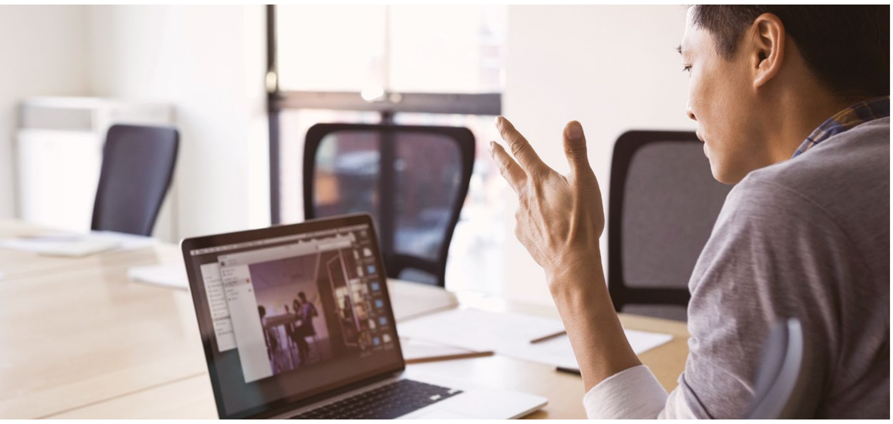
Cyber resilience solutions: How we can help

Our cyber resilience team has extensive experience working with organisations in a broad spectrum of security functions and have effectively delivered end to end cyber resilience programmes.

Organisations need to have proven strategies to effectively deal with disruptive events. By partnering with us, we can better prepare and assess the readiness of your organisation to face the challenges that these disruptive events create.

There are five key factors which we can implement to improve your organisation's cyber resilience:

- Assess how effective your current systems are and identify key risks
- Identify critical systems and processes at risk of attack, then implement changes which will reduce the potential disruption to your business
- Review third party risk management arrangements. Identify and appropriately manage the resilience risks arising from those arrangements
- Make sure that current systems comply with industry, regulatory and legal standards
- Create multi-year, on-going programmes to preserve and enhance the effectiveness of your privacy and cyber security systems



Our cyber resilience offerings

Our cyber resilience team consists of highly specialised professionals with extensive experience of key areas, including:

- Cyber crime
- Business continuity
- Crisis management
- Third party risk
- IT disaster recovery
- Incident management
- Resilience benchmarking
- Training, education and exercising
- Governance, risk and compliance

Case Study

After suffering from a high number of disruptive cyber incidents and events, the client, a leading insurance provider, requested specialist expertise regarding their cyber and information security risks and the suitability of their relevant controls. We reviewed information security policies, processes and practices. It was also necessary for us to identify security requirements driven by regulation, perform a gap analysis to identify weaknesses and agree recommendations. Based on this, enhanced controls over user access could be implemented, as well as control and supplier management. Current policies were benchmarked with international standards and peers. We supported the client through the demonstration and application of both risk based methodologies and approaches to focus on material risk exposures, and supported the client with improving control maturity.

About us

Grant Thornton UK LLP is the UK member firm of Grant Thornton, one of the world's leading international organisations of independently owned and managed accounting and consulting firms. Over 47,000 Grant Thornton people, across 130 countries, are focused on making a difference to clients, colleagues and the communities in which we live and work.

Grant Thornton's cyber security and privacy team has significant experience of assessing, improving and embedding controls to better align exposure and risk appetite. The cyber security and privacy team have worked with a range of organisations, varying in size and industry, so we are well equipped to tailor our services to meet specific client needs.

Our experience in cyber resilience and privacy covers a wide range of topics, including cyber security, cyber crime, digital security, vendor assurance and data privacy.

Contacts

Sandy Kumar
Chair of Financial Services Group
Head of Business Risk Services UK
Advisory
T +44 (0)20 7865 2193
E sandy.kumar@uk.gt.com

Manu Sharma
Head of Cyber Security
Financial Services
Business Risk Services
T +44 (0)20 7865 2406
E manu.sharma@uk.gt.com

Kev Brear
Head of Resilience Services
Financial Services
Business Risk Services
T +44 (0)20 7865 2425
E kev.brear@uk.gt.com

Grant Thornton
An instinct for growth™

grantthornton.co.uk

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.

GRT105911