Security Risk Management

CYBERFORT

By 2022, at least 95% of cloud security failures will be the customers fault, Gartner 2019

As business data becomes an increasingly valuable source of competitive advantage, it's also becoming a more attractive target for cybercriminals. An effective security risk management strategy will give you a resilient security posture to safeguard your valuable assets and help your business succeed and grow.

Cyberfort's experts will carefully analyse the impact of possible future events that might threaten your business. We'll collate and present our analysis of your business risks in an understandable, pragmatic way, giving you a holistic, organisation-wide view of your entire risk landscape.

Armed with a clear understanding of your security risks, you'll be able to devise and implement plans in a deliberate, responsible and ethical manner, making decisions that are right for your business. This service will help you demonstrate cyber resilience to key stakeholders (your executive board, shareholders, customers, insurers and regulators for example.)

Cyberfort's expert teams will examine risks in deep granular detail, deploying risk, threat and vulnerability assessments to identify weaknesses associated with your people, processes and technology. Cyberfort will further support in design and development of appropriate and pragmatic security controls, helping you meet your regulatory and compliance obligations.

For more information please contact us on:
T: 01635 015600 E: info@cyberfortgroup.com

Security Risk Management

Cyberfort will design a roadmap and implement strong information security governance processes to help you manage risk now and in the future. Our risk management solutions are designed to be strategic, pragmatic and cost-effective, and to create a security-aware culture. We align the service to your particular business needs and strategic objectives. Your security risk management service can include:

- Asset Discovery
- Threat Identification
- Strategic Risk Assessment and Management
- Business Continuity and Disaster Recovery
- CISO/Cyber Strategy
- Cyber Assurance and Audit
- Cybersecurity Project and Programme Management
- Information Security Awareness and
- Training Programmes
- Cyber Investigation Diligence (CID)
- Governance and Regulatory Compliance
- Supply Chain Assurance

Maintaining cybersecurity and resilience is a continuous, iterative process. As threats and attacks evolve, so must your security processes. If a successful attack does occur, Cyberfort will support you by helping to recover business operations and keep services essential to business continuity and growth running. Cyberfort identifies critical business functions and processes, then delivers continuity and disaster recovery solutions specific to your business. This ensures that if the worst happens, consequences are managed, and impacts are minimised.

Cyberfort has established a strong reputation in both the public and private sectors for delivering robust, tailored risk management solutions to clients ranging from large multi nationals and public to SMEs and tech startups. Cyberfort's teams have many years of experience and hold professional certifications that include:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- ISO 27001 Lead Auditor and Implementer
- National Cyber Security Centre (NCSC)
- Senior certified CCP Security and Information Risk Advisors
- Certified in Risk and Information
- Systems Control (CRISC) Practitioners
- PCI DSS Certified
- CPNI Accredited Site Security Auditors

Cyberfort follows international guidance including NCSC, DOD, MOD and international best practice.

Our specialists assess risk against recognised compliance regimes and frameworks including ISO27001 and NIST. Our approach to helping businesses is agile, offering a thoughtful, bespoke approach tailored to your specific needs. Our security risk management service is never a 'tick-box' exercise. We translate the risks you face into clear, business specific language. Cyberfort keep businesses secure today while also focussed on future priorities and your evolving requirements.

Your Security Risk Management challenges

The ability to identify, detect, respond and recover is vital to ensuring an organisation survives in today's evolving threat landscape. Cybersecurity issues you may be facing include:

- Increasing cyber threat - nearly a third of businesses report having cybersecurity breaches in the last 12 months
- Increasing legal and regulatory pressures
- Changes in how people do business. The increasing use of digital and cloud services is introducing new risks that need to be addressed
- Compliance and regulatory requirements introduce added time pressures and complexity into businesses, while implementing security controls increases costs
- Lack of experienced cybersecurity and risk management expertise is putting pressure on internal resources who don't have the necessary skills
- Lack of awareness or inadequate security training
- New threats and methods used by criminals mean security needs to continually evolve

How Cyberfort can help you

The ability to identify, detect, respond and recover is vital to ensuring an organisation survives in today's evolving threat landscape. Cybersecurity issues you may be facing include:

- Achieve clear tangible return on investment (ROI) by enabling your organisation to make prioritised and informed business decisions
- Drive operational efficiencies through process improvements
- Invest in cost-effective solutions based on our expert guidance in accordance with your risk profile
- Understand risks in the context of business activities and growth, minimising potential impact if risks are realised
- Achieve full strategic oversight, allowing you to effectively manage security risk and compliance
- Embed a culture of security awareness and establish efficient organisation-wide training programmes
- Ensure business objectives are aligned with your organisation's risk appetite
- Benefit from our expert guidance on security strategy
- Ensure your security strategy aligns with your corporate obligations to protect personal and sensitive data, compliance with regulatory requirements and frameworks
- Strengthen the maturity of your processes and information security governance
- Identify and assess critical assets, obtaining assurance that the appropriate technical and organisational measures are in place to protect them