Cyber Risk Management

The growth in cloud services, the rise of remote work, and the increased reliance on third-party IT service providers has meant more people, more devices, and more software on the average company's infrastructure. As an IT system grows, so does its attack surface and its vulnerability.

All organisations depend on information technology to do business today, exposing them to cybercriminals, employee errors, and other cyber security threats. These threats can take critical systems offline, leading to lost revenue, stolen data, long-term reputation damage, and regulatory fines.

Cyber risk management initiatives offer organisations a way to identify and manage their evolving attack surfaces, improve their security posture and ultimately protect their information.

Improve your defences with risk management

Risks can't be eliminated completely, but cyber risk management programs and services can limit the impact and reduce the vulnerabilities. In many cases it is both a business imperative and a legal mandate to undertake some form of risk management assessments, as regulations oblige organisations to protect certain types of information.

Companies can use cyber risk management output to then target their most critical threats and choose the right IT security solutions to defend themselves based on their business priorities.

Without a full understanding of the risks to your business you may suffer:

- **Reputation damage**
  A perception of inadequate cyber security measures may drive customers away, leading to lost revenue and market share. Competitors perceived as more secure may gain an advantage, affecting your organisation's financial performance.
- **Potential withdrawal by the regulator of your license to operate**
  Regulatory actions can have severe consequences. It may disrupt business operations, cause financial losses, and tarnish your standing in the industry.
- **Financial penalties**
  Substantial financial penalties can significantly impact your bottom line. Organisations may face steep fines, leading to financial strain, potential bankruptcy, or a substantial reduction in profitability.
- **Loss of data**
  The loss or corruption of contact data can result in direct harm to customers and partners. It may lead to communication breakdowns, privacy concerns, and potential legal consequences, damaging relationships and business operations.

Regardless of the size, every organisation has one thing in common: information. Information comes with responsibility. Organisations must protect the information itself, inform the behaviour of those carrying the information, have visibility regarding where their confidential data resides on their network, have influence over where that data is going, and implement a policy for managing it. A strategy that balances the organisation's legal and business needs to protect information is vital.

Now is the time to revisit what information you have, where this resides, and the necessary steps needed to protect it.

Cyber Health Check

Cyber hygiene is the best step towards preventing any kind of security breach. With cyber threats to businesses increasing daily, the need for external specialists to check the status of your IT risk is vital to tackle the problems today's technology can bring.

Cyber Health Checks should be carried out as often as you can but should be at least twice a year – we recommend four times a year. We interview your key stakeholders, review the evidence of your cyber security hygiene, and provide you with a written assessment of your maturity level across multiple domains, aligned to the Cyber Security Body of Knowledge (CyBOK) knowledge areas:

- Human, organisational & regulatory aspects
- Systems security
- Software and platform security
- Infrastructure security
- Attacks & defences

Areas of assessment include:

- Planning and risk management
- User education and awareness
- Employee screening & responsibilities
- Supplier security management
- Contingency planning
- Legal and other external requirements
- Removable media use
- Logical access control
- Secure configuration
- Remote working and mobile devices
- Management of assets

Cyber Health Checks can include:

- **NIS2 Directive**
  The Network & Information Systems (NIS2) Directive provides regulations to increase cyber security and resilience levels of vital systems across the EU, impacting various different organisations within multiple industries. It establishes a baseline level of security for network and information systems, addressing threats posed to the economy and society in general. Resillion offers advice and support to those who must comply with the NIS2 Directive.

- **Standards Implementation & Management**
  Looking to achieve an industry standard but not sure where to start? Resillion will guide you through every step of the process, including understanding your current level of compliance and the necessary steps involved to get you exactly where you need to be.

- **Cyber Due Diligence**
  Cyber risk goes further than what's right in front of you. We'll examine your entire portfolio and identify any current or future risks to your business operations and other crucial stakeholders.

- **Cyber Essentials**
  Safeguard your organisation against common cyber threats. We'll help you to demonstrate that your commitment to cyber security meets government standards. Protect yourself against modern threats, like hacking and phishing, and become aware of external vulnerabilities and how to resolve them.

- **Supply Chain Auditing & Assurance**
  Given the escalating threats posed by hackers, it's crucial to acknowledge that your organisation could be targeted through your partners and suppliers. We'll review all the processes across your entire ecosystem.

- **Resource augmentation**
  Partner with an expert third-party for cyber support and bridge your resource gap exactly when you need it, mitigate cyber risk, and meet your business objectives.

CISO as a Service

CISO turnover is one of the largest in the business. This together with the difficulty in recruiting, paying for and then managing a security environment is too much for many businesses. What our service provides is invaluable expertise from an outsourced CISO. Our service helps you manage risk effectively, maintain your information security systems, and enhance your current security capabilities.

Our Chief Information Security Officer (CISO) Service bridges the gap between the board, business, and operational security through their expertise in management, governance, and information security. They can support with the implementation and management of ISO 27001, NIST Cyber Security Framework and other best-practice frameworks or support business, technology, and cyber transformation. A delegated CISO becomes a credible representative to interact with the C-suite, external stakeholders, and investors.

DPO as a Service

Meet your data protection, privacy, and information security compliance requirements, in accordance with the GDPR with the help of an outsourced Data Protection Officer. Get practical advice and expertise on the latest trends, best practice, and regulations today.

Data Protection & Privacy Consulting

Data protection and regulatory requirements are at the forefront of your business operation. Many organisations struggle to understand accountability and privacy by design, including the effects on e-privacy and other regulatory requirements. With the help of an expert consultant. Resillion supports you from policy development, to implementation, protecting your organisational risk and compliance. We can help you comply with a range of international data protection and privacy laws from a global perspective.

Our team of international subject matter experts help you to navigate complexity and establish your current level of compliance, identifying necessary steps to achieve and address any areas which need to comply and support you in implementing necessary policy, process, and documentation.

We provide:

- Regulatory compliance gap analysis and roadmap – identify gaps in your current stance against compliance requirements of specific standards and legislation and provide recommendations.
- Implementation workshop – prepare for the work required to achieve and maintain compliance and create a program and roadmap.
- Virtual Data Protection Officer – a subject matter expert with specialist knowledge and business experience, able to advise on requirements, legal compliance, implementation, and operation as well as specific items like conducting complex Subject Access Requests.

By understanding your data protection obligations and how personal data is used, stored, and processed throughout your organisation, your ability to mitigate risks to the confidentiality of this data is greatly improved.

Threat Modelling

Regular threat modelling keeps you one step ahead of the constant changes surrounding your organisation. One of the largest damaging problems is IT drift where configurations and assets constantly change. Regardless of your maturity, Resillion will support you throughout the entire process or provide an objective perspective at the times you need.

Threat modelling takes a step back from traditional cyber security approaches, taking a broader view to consider anything that could a negative impact on your organisation. Using the MITRE ATT&CK Framework as a basis, we build on this to uncover threats that might have otherwise gone unnoticed, or not properly accounted for and by taking a proactive approach, threats are addressed before they turn into bigger issues.

All advice is tailored to your organisation, thanks to expertise grown through working with various industries. Threat modelling should be weaved into your development lifecycle to improve the end result.