LATERAL
CONNECT

The Importance of Cybersecurity Training to Ensure Business Continuity

Improve Cyber Resilience and Protect your Reputation

www.lateral-connect.com

With recent data breaches leading to regulatory fines, other technical issues, litigations or class action lawsuits, they all enforce the importance of the modern enterprise to be agile and to rapidly adapt their security strategies.

Cyber resilience vs. Cybersecurity

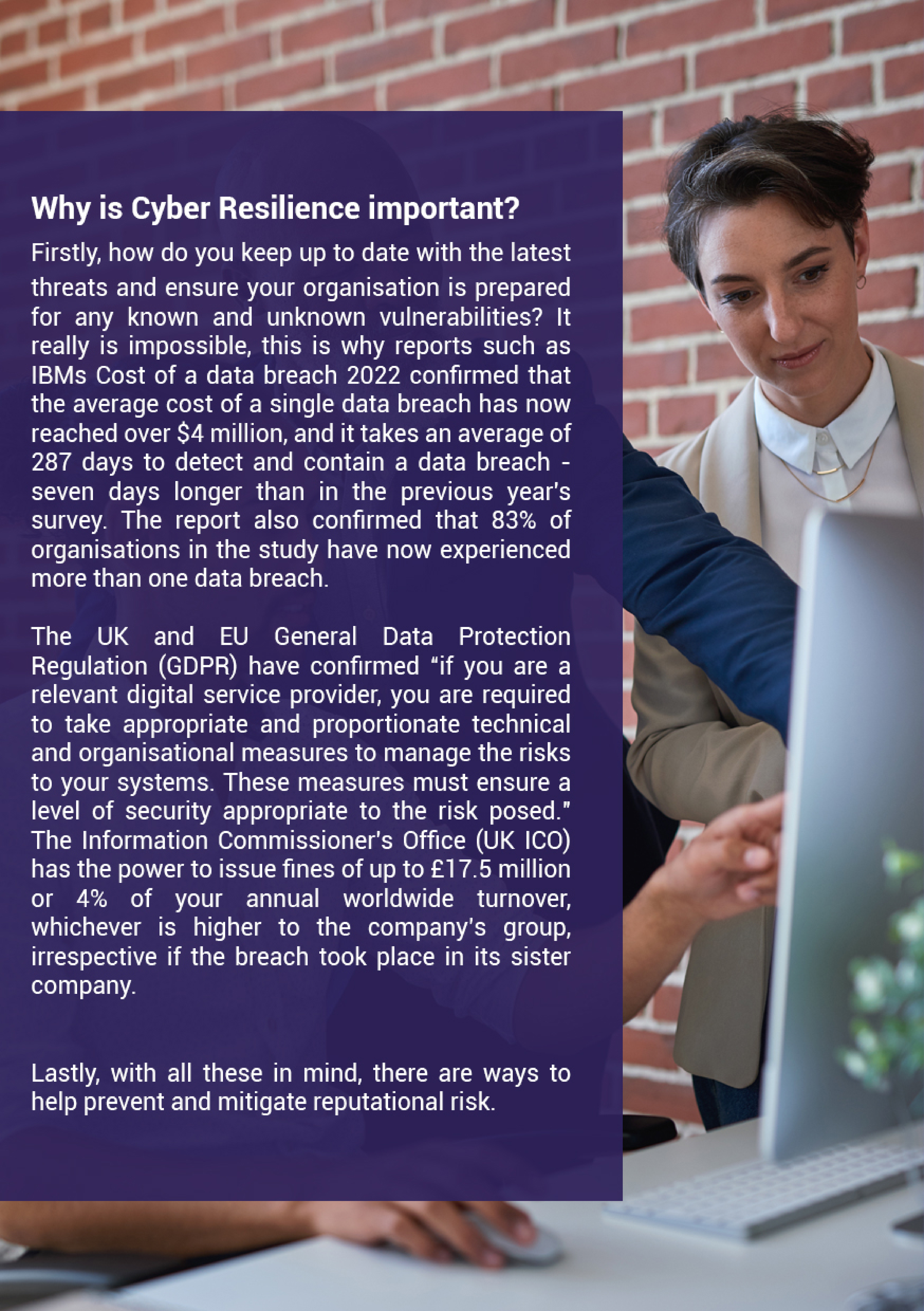
Cyber Resilience

The ability to limit the impact of security incidents by deploying and optimising appropriate security tools, your people and your processes. Cyber resilience also includes the ability to continuously strengthen your overall cyber defences in the face of adverse cyber threats, and learning from yours and other organisations past and present data breaches.

Cybersecurity

Having a cyber defence strategy which consists of technologies, people and processes that are designed to enforce policies and protect systems, networks, data, and IT infrastructure from cyber threats (e.g., malware, ransomware, hacktivism, malicious insiders).

Both of these are equally as important as one another, and will support and help strengthen an organisations business and cybersecurity strategy against cyber threats.



Why is Cyber Resilience important?

Firstly, how do you keep up to date with the latest threats and ensure your organisation is prepared for any known and unknown vulnerabilities? It really is impossible, this is why reports such as IBMs Cost of a data breach 2022 confirmed that the average cost of a single data breach has now reached over $4 million, and it takes an average of 287 days to detect and contain a data breach - seven days longer than in the previous year's survey. The report also confirmed that 83% of organisations in the study have now experienced more than one data breach.

The UK and EU General Data Protection Regulation (GDPR) have confirmed “if you are a relevant digital service provider, you are required to take appropriate and proportionate technical and organisational measures to manage the risks to your systems. These measures must ensure a level of security appropriate to the risk posed." The Information Commissioner's Office (UK ICO) has the power to issue fines of up to £17.5 million or 4% of your annual worldwide turnover, whichever is higher to the company's group, irrespective if the breach took place in its sister company.

Lastly, with all these in mind, there are ways to help prevent and mitigate reputational risk.

How to Improve Cyber Resilience

There are a number of steps that organisations can take to improve cyber resilience, by using the NIST Cybersecurity Framework. These include (but are not limited to) the following:

IDENTIFY

Develop and manage cybersecurity risk to systems, assets, data and capabilities by carrying out:

- a gap analysis against a security framework or security standard that aligns with your business goals and objectives
- a risk assessment to identify your critical assets and define your KPIs (key performance indicators) and KRIs (key risk indicators) to hold your teams to account
- a categorising matrix of all your assets, including supplier chain relationships i.e your personal, sensitive and financial data and manages it a risk management strategy that is easy to understand and follow

PROTECT

Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services by:

- purchasing a data loss prevention (DLP) tool

- automating your access control process using JML (joiners, movers and leavers), including admin rights and elevated admin rights i.e. least privileged, need to know etc.

- creating a cybersecurity training and awareness strategy for your users and technical teams

- creating relevant user policies and procedures, as well as technical teams documentations i.e. acceptable use policies for users and firewall configurations guides, business impact assessment (BIA), disaster recovery plan (DRP) for technical teams

- reviewing and testing your business continuity plan (BCP), your DRP and BIA on an annual basis, after a significant change or after an incident or data breach is recommended

DETECT

Develop and implement appropriate activities to identify and monitor the occurrence of cybersecurity event by:

- having a Security Operation Center (SOC) to carry out the following logs, such as security devices, network components, applications, servers etc.

- considering using artificial intelligence (AI) to monitor IT systems and networks to detect security threats, performance issues, behavioural changes, or non-compliance problems in an automated manner

- considering to detect: Anomaly-Based Intrusion Detection, Hybrid Intrusion Detection and Signature-Based Intrusion Detection

RESPOND

Develop and implement appropriate activities to take action regarding a detected cybersecurity event by carrying out:

- ensuring your BCP and DRP are up to date and fit for purpose
- ensuring you have a crisis management communication plan that is tested annually and ensuring the stakeholder details are up to date
- ensuring incidents, problems and data breaches are correctly mitigated and lessons learnt documentations in place and processes and procedures updated

RECOVER

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event by:

- having a recovery plan, including related processes and procedures in place
- ensuring key stakeholders details, including supply chains are in place for those who are relevant and critical in your recovery plan
- reviewing if any of the technology's, people or process did not identify a threat
  - identify any training and awareness or updates to the technology
- review lessons learnt and categorise it, to help identify any gaps in your technology, your processes and your people

Final Thoughts

It is evident that organisations continue to overestimate their resilience capabilities,while many possess an awareness of the importance of resilience, however, there is an unwillingness to invest in or execute preventative measures or have the notion of ‘it will never happen to them…just yet’.

It’s no longer a matter of ‘if’ but ‘when’ an organisation will suffer a cyber attack. This means, it’s better to assume threat actors will eventually break through your defences, so it is beneficial to start working on a strategy to reduce the impact.

Successfully managing cyber resilience is necessary as organisations and executives face fines and other serious consequences. Potential repercussions mean board members must understand cyber risks and the best ways to mitigate them.

LATERAL CONNECT

Written by a Security Trainer @lateral-connect.com