daisy.

Building Cyber Resilience:

Practical Guidance for Defending your Organisation

What being ‘Cyber Resilient’ looks like in practice

Being cyber resilient means having the ability to anticipate, withstand, quickly recover from, and adapt to adverse conditions or cyber attacks whilst maintaining business operations.

Disaster recovery and business continuity are related concepts, but they differ in their focus. Disaster recovery refers to an organisation’s ability to restore IT systems and data in the event of a major disruption, such as a power outage or hardware failure. Business continuity involves ensuring that an organisation can continue operating its critical functions in the face of disruption. Both concepts are incorporated into the latter stages of the cyber security framework – namely ‘Respond’ and ‘Recover’.

While there is some overlap between cyber resilience, disaster recovery and business continuity, it is important to note that being cyber resilient requires a proactive and adaptive approach to cyber security. One that is tailored to the specific needs and risk appetite of an organisation. This involves a combination of people, processes and technology to protect against cyber threats and respond effectively when incidents occur.

Building Cyber Resilience:

Practical Guidance for Defending your Organisation

Start with risk management, not technology

It is a common misconception that being cyber resilient is simply having a range of Gartner Magic Quadrant 'Top Right' technical security controls deployed and then sitting back and relaxing, safe in the knowledge that the best tech will stop the most threats. The reality is that even with so many vendors and solutions on the market that afford protection against certain attack vector scenarios, there is still no silver bullet.

Before even considering technical security controls and potentially blowing your budget on the best firewall available to protect your network (and not having enough left to secure your email system or your endpoints), organisations are recommended to take a risk-assessed approach. This will allow them to make informed and improved decisions as to the highest risk assets that need protecting against specific threats.

Risk management can be complex, but it doesn't have to be. Organisations who only utilise bring your own device (BYOD) and software as a service (SaaS) may quickly decide that they are happy with the cloud provider's security controls and see the biggest threat being their CEO or CFO clicking on a 'bad' website link embedded within an innocent looking, and seemingly legitimate email. A financial organisation which hosts their own data centres but allows their staff to work in a shared office building with shared network infrastructure utilising a lot of external and temporary contracting staff, may need to take a more structured and detailed approach. This requires a robust cyber security strategy that encompasses a wide range of security measures.

Developing an understanding of the business context, the resources that support critical functions, and the related cyber security risks, enables an organisation to focus and prioritise its efforts. **This is commonly known as the 'Identify' stage.**

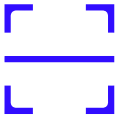
Stopping the bad guys

Developing and implementing appropriate safeguards to ensure the delivery of critical assets is all about rolling out identified preventative security controls during what is **commonly known as the 'Protect' stage.** Examples include:

- Using a firewall to secure your internet connection
- Using secure settings for your devices and software
- Controlling who has access to your data and services
- Protecting yourself from viruses and other malware
- Keeping your devices and software up to date
- Scanning your network, applications, and devices for vulnerabilities and weaknesses
- Developing and implementing an acceptable use policy for all users

Building Cyber Resilience:

Practical Guidance for Defending your Organisation



Accepting that the bad guys will (sometimes) be successful

As mentioned above, there is no silver bullet – the bad guys will always keep on trying to break into your systems and are often well ahead of cyber security vendors as they identify new ways in which to facilitate the success of their nefarious activity. If you don't know a breach has taken place, then over a period of months (potentially years), the bad guys could secretly be stealing your data or they may have installed 'Trojan Horse' ransomware for activation at a more opportune time for them. Examples of reactive technical security controls during this **'Detect' stage** include:

- A centralised security information and event management (SIEM) platform to collate event log data (from multiple different and disparate IT and security systems) that indicates a compromise or breach is likely, and needs further investigation by skilled security analysts
- A user and entity behaviour analytics (UEBA) tool that identifies user activity that is unusual for a specific user and the manner in which they usually access organisational data and IT systems
- Endpoint detection and response (EDR) to detect and respond to advanced threats facing endpoints and servers
- Skilled security analysts (as part of a wider security operations centre's (SOC) function) to investigate, triage, and make recommendations for appropriate remediation activity in line with the wider incident response plan
- A vulnerability management solution to identify, categorise, and prioritise the remediation or mitigation of vulnerabilities across your IT infrastructure

Stopping the bad guys from having too much fun

So, the bad guys are in, which is of course bad news. However rather than the glass being half empty, it is in fact half full as at least you know about it and are empowered to do something about it during **the 'Respond' stage.** Whilst certain activities only take place after an incident has been confirmed, the associated remediation activities firstly need to be developed before they can be implemented. Effectiveness at this stage is entirely dependent on detailed plans having firstly been made. Examples of relative activities include:

- **Incident Response** - Having an incident response plan in place ensures that organisations can respond to a cyber security incident quickly and effectively. It is important that businesses perform regular testing of their incident response plan, so that your staff know what they need to do and take it in their stride when the time comes.
- **Backup & Recovery** - Enables organisations to quickly restore their systems in the event of a cyber security incident. This involves regular data backups, and testing your disaster recovery plans.
- **Business Continuity** - The importance of having an over-arching plan to continue business operations that is wider than the incident response and IT protection and availability cannot be underestimated.

Building Cyber Resilience:

Practical Guidance for Defending your Organisation

Returning to normality

This final 'Recover' stage is focused on reducing the impact of a cyber security incident by restoring any capabilities or services that have been impaired or are even completely unavailable. Examples of relative activities include:

- **Implementing the plan** - Recovery processes and procedures are executed and maintained to ensure restoration of affected systems and assets
- **Effective communication** - Restoration activities are coordinated with all relevant parities – both internal and external
- **Lessons learned** - Improvements are facilitated by incorporating lessons learned into future planning and actions

Looking to the future

The **'Govern'** stage serves as the cornerstone for aligning cyber security efforts with organisational objectives and stakeholder expectations. Some of the challenges for effective cyber governance are:

1. Gaining senior leadership acceptance and understanding of cyber resilience goals and strategy
2. Ensuring a robust framework, that is understood across the organisation, with input and engagement from key stakeholders from across all potentially impacted departments
3. Maintaining consistency and accountability among stakeholders, reinforced by regular scenario testing
4. Securing adequate resources, via investment from both a financial and skilled personnel perspective

In navigating the complexities of cyber security governance, organisations often benefit from expert guidance and support, including:

- **Virtual CISO services** - For businesses lacking cyber leadership or looking to establish an implement an effective cyber security strategy
- **PCI DSS compliance -** To ensure the secure handling of payment card data and reduce the risk of data breaches
- **ISO 27001 certification** - For organisations looking to demonstrate their commitment to robust information security management systems
- **Cyber Essentials accreditation** - Guiding organisations through the Cyber Essentials accreditation process to establish fundamental cyber security measures that help protect against common online threats
- **Cyber Security Review** - Understand the current risk exposure and help build a prioritised approach to addressing those risks

Building Cyber Resilience:

Practical Guidance for Defending your Organisation

Conclusion

Cyber security is about protecting your network, your data, your customers and your reputation. The financial and reputational damage caused by data loss and downtime can have a huge, even devastating impact.

Our modern business world is dynamic, complex, and continually evolving. So are the security threats associated with conducting business and interacting with the world online. It is now a common belief that it's not "if" but "when" you will face a cyber attack – no organisation is immune.

This means that your security strategy needs to be robust, multi-layered and able to evolve to keep you up to date with the risks that you face. Cyber security is not just important, it is essential.

If you want to find out how Daisy can help you to improve your security posture, contact us on:

0344 863 3000