Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Cyber Security is A Business Challenge

Not simply a technical hurdle for the IT crowd

Audience: General **Reading Time: 5 Mins**

As we move further into the age of digital globalization cyber security has emerged as a pressing concern for anyone that uses digital technology. Business leaders must move away from the idea that such concerns are confined to IT departments, and recognise the duties extending to senior management.

In this context, SMEs face a unique set of strengths and limitations. This article aims to analyse those factors, arguing that cyber security, far from being merely a technical hurdle, is in fact a fundamental business challenge that calls for comprehensive strategies to mitigate threats effectively.

Strengths and Limitations of SMEs:

Let us first consider the strengths of SMEs in managing cyber security. Small and medium-sized businesses are known for their agility and adaptability - characteristics that can give them an advantage in responding to cyber threats. With flatter organisational structures and less bureaucratic inertia, they are often able to respond and adapt to security incidents far more quickly than their larger counterparts.

Despite these advantages, the constraints that SMEs face are significant and, in many cases, disproportionately greater than those faced by larger corporations. Primarily, SMEs typically operate with more limited resources – both financial and human. SMEs are often unable to afford the high cost of employing full-time cyber security professionals or engaging third-party security vendors. Consequently, they often rely on employees with basic technical knowledge, who may lack the requisite expertise to effectively defend the organisation against sophisticated cyber threats.

Another limitation is the widespread perception that SMEs are "too small to be targeted". This misbelief leads to complacency, with SMEs failing to implement robust security measures. The truth is, cybercriminals often specifically target SMEs, precisely because their defences tend to be weaker.

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University
MANCHESTER 1824 The University of Manchester
Manchester Metropolitan University
University of Salford MANCHESTER

Finally, the increasing trend of remote work, brought on by global events such as the COVID-19 pandemic, has created additional security vulnerabilities. For SMEs with a distributed workforce, ensuring secure access to data and systems, becomes increasingly complex.

A Business Challenge, Not A Technical One

Having recognised the strengths and limitations of SMEs in the realm of cyber security, let's shift our focus to understanding why this issue is a business challenge and not merely a technical hurdle. A successful cyber-attack can have profound consequences, not just on the operational level, but strategically and financially. The impact of data breaches, ransomware attacks, and other cyber threats can disrupt business operations, damage reputations, erode customer trust, and result in significant financial losses.

Furthermore, SMEs' suppliers, customers, and partners increasingly demand proof of robust cyber security measures. Thus, cyber security has become a prerequisite for business transactions and collaborations, making it a business issue rather than a mere technical one.

Mitigating Cyber Threats

Given the gravity of the threat landscape, SMEs must take a proactive stance in combating cyber risks. Some strategies to consider:

Risk Awareness and Education: Ignorance breeds complacency. SMEs need to be aware of their cyber risk landscape and educate their workforce on best practices for digital hygiene. This includes training on recognising phishing attempts, using strong, unique passwords, and understanding the importance of regular software updates.

Institutionalise Cyber Security: Make cyber security an integral part of business strategy and operations. This means regularly reviewing and updating cyber security policies, ensuring secure configurations, backing up data regularly, and encrypting sensitive information.

Leverage Affordable Tools: There are affordable and effective cyber security tools available, such as antivirus software, firewalls, and intrusion detection systems. Use them to protect your systems and data.

Incident Response Planning: Prepare for a security breach by having an incident response plan. This includes identifying a response team, outlining communication strategies, and establishing a recovery plan.

Collaboration and Outsourcing: Consider collaborating with other businesses or outsourcing certain security functions to managed security service providers. This can provide cost-effective access to professional expertise.

Cyber Insurance: As a safety net, consider purchasing cyber insurance. This can help cover the financial impact of a cyber-attack, giving your business a chance to recover. It should be noted that becoming accredited with Cyber Essentials, a scheme backed by the NCSC, comes with its own cyber insurance.

Finally, in an increasingly interconnected digital world, cyber security is no longer optional for SMEs—it is a business necessity. As they navigate their digital transformation journey, SMEs must prioritise cyber security, leveraging their unique strengths, and overcoming their limitations, to adopt a comprehensive and proactive approach to managing cyber risks.

By viewing cyber security as a business challenge rather than just a technical hurdle, SMEs can turn this challenge into an opportunity—enhancing their resilience, building trust with customers and partners, and securing their competitive edge in the digital marketplace. Ultimately, cyber security is not only about protecting the business from threats, but also about enabling its growth, innovation, and long-term success.