The problem

Research shows that **SMEs aren't** as **concerned** as big corporations when it comes to the **cyber threats** they face every day – a KPMG and Be Cyber Streetwise survey[1] found that

of small businesses "think it's **unlikely or very unlikely that they'd be a target for an attack**".

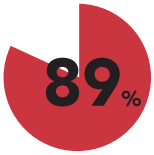
SMEs are really attractive to cyber criminals because:

- they have **poor security** measures in place;
- they have **limited resources**;
- they are **part of larger supply chains** – they are exploited as back doors into larger corporations' systems.

The reality is that they are **as much at risk as big companies** – the only difference is that security breaches are likely to have a higher cost for large companies. The average cost of the worst cyber attack to large organisations is £1.46m - £3.14m, compared to £75k - £311k for small businesses.[2]

Can your business afford to lose up to £311k on something you could have prevented?

The biggest risk is reputational damage:



of breached SMEs said the attack affected their reputation.

Reputational damage comes in many forms:

Brand damage

A cyber attack of any magnitude will affect a company's ability to continue operating. It takes an average of 26 hours to recover from an attack. During this time, respondents to the KPMG survey listed the following:

32% had to pay someone to fix the issue;

26% experienced customer delays;

21% were forced to shut down their website;

20% incurred legal costs.

Even if a company can fix the issue in a day, it usually takes over six months to fully recover and get back on track.

Ability to attract new employees

Staff are not safe from the effects of a data breach either:

of SMEs said their employees were affected with 29% experiencing "stress and concern" and 27% worried about the "loss of their personal data".

Ability to win new business

Suppliers want to be reassured that cyber security best practice is followed:

of procurement managers say that **cyber security standards are important** when awarding a project to a potential supplier.

Loss of clientele

Customers are increasingly concerned about how companies store and protect their sensitive data.

of consumers said that knowing a company had been breached would discourage them from using its services.

What should worry companies about this statistic is the impact of word of mouth: unhappy customers are very likely to share their bad experiences with their family, friends and colleagues. In the age of social media, this message will spread fast, and bring with it the risk of being picked up by the media and even ending up in the news.

Adopt the Cyber Essentials scheme to protect your data and business

The Cyber Essentials scheme provides five security controls that, according to the government, **could prevent "around 80% of cyber attacks"**.[3] It is a mechanism that organisations can use to demonstrate to customers, investors, insurers and others that they have taken essential precautions to secure their information against the majority of cyber risks. The scheme's five security controls provide a basic level of protection from the vast majority of cyber attacks so that you can focus on your core business objectives.

CYBER ESSENTIALS

Implement these five controls to strengthen cyber security AND improve business efficiency

1. Secure configuration

Cut costs on systems or databases that you no longer need or use
Developing a consistent software installation and configuration management process or system enables you to easily understand the resources you use – and those you don't – so that you can dismiss the most outdated ones and cut costs on maintenance and storage.

Identify bottlenecks
Identifying outdated resources gives you the opportunity to discover bottlenecks – a lack of computers or software undermining your company's daily business. Fixing these can provide greater business efficiency.

2. Boundary firewalls and Internet gateways

Cut costs on your bandwidth requirements
Firewalls and gateways identify and block unwanted traffic that could be harmful to your computers, systems and networks, helping you to understand and manage your bandwidth requirements, and thereby allowing you to renegotiate your hosting costs.

Learning curve
Identifying the cyber attacks that target your company allows you to create an internal database that can inform how you recover from them and how to prevent attackers from accessing your network in the future.

3. Access control and administrative privilege management

Optimise your staff workload and time
By restricting admin access to applications, computers and networks to a small group of users, you are in control of what can or can't be installed on company computers. Staff should be given the lowest access level necessary to their job functions in order to avoid the installation of harmful, unnecessary or time-wasting software.

Cut costs on software licences that you don't need
Staff should be given access to the software and applications they need to perform their tasks; any other access is unnecessary. As a consequence, you can save money on superfluous software licences.

4. Patch management

Increased productivity
Patches improve software performance and remove the issues that slow down employees, such as software crashes and poor performance caused by congested networks.

5. Malware protection

Time and cost savings on recovering infected devices
Infected devices cost you time and money when they're out of action: there's the cost of repair and the cost of substitute devices, as well as the fact that your technical staff would doubtless be better utilised. With a malware protection system in place, you avoid such costs.

IT Governance's **CyberComply portal** has made the journey from cyber insecurity to assured cyber security as simple as possible! Read more: www.itgovernance.co.uk/cyber-comply.aspx

Cyber Essentials certification is well within your reach

Whatever your organisation's cyber security budget or level of technical expertise, achieving certification is well within your reach. The journey starts with identifying the scope of your certification; the next step is to submit the self-assessment questionnaire through the unique CyberComply portal; finally, let IT Governance conduct an external vulnerability scan of your network and applications. When you pass the assessment, you will be awarded the Cyber Essentials or Cyber Essentials Plus badge to demonstrate that you achieved certification.
See the infographic for a better understanding of the journey »

Cyber Essentials certification advertises the fact that you are following government-endorsed standards for cyber security, and that you protect the privacy of your customers, suppliers and stakeholders.

The most straightforward and convenient way to get started and achieve certification is with our Cyber Essentials – Do It Yourself packaged solution: we will assess how successfully you have implemented the five controls, we will scan your network and system for vulnerabilities, and, if everything is satisfactory, we will award you a Cyber Essentials certificate – all for just £300.

Get started from just £300 »

If you need more help getting cyber secure, you might be interested in our Cyber Essentials - Get A Little Help or Cyber Essentials – Get A Lot Of Help packages. Both packages provide you with tools, resources and specific advice on how to tackle cyber security.

We let our happy customers speak for us:

"We are delighted to have achieved this certification in Information Security. As a business Status are committed to providing our clients with the highest level of data protection, and this accreditation clearly demonstrates that focus."

Graeme Wilkinson, technical director – Status Digital Marketing Ltd

"By achieving this Cyber Essential Plus certification we demonstrate to our customers that ELEXON has robust practices and policies which protect us from cyber-attacks."

Nigel Smith, CFO and director – Professional Services of ELEXON Ltd

[1] https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf
[2] https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf
[3] https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms

IT Governance Ltd
Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs CB7 4EA, United Kingdom

t: + 44 (0) 845 070 1750
e: servicecentre@itgovernance.co.uk
w: www.itgovernance.co.uk

@ITGovernance /it-governance /ITGovernanceLtd