

ENTERPRISE

A SECURE FUTURE

UNDERSTANDING AND REDUCING RISKS WITH A CYBER SECURITY AUDIT



0345 565 1767

info@intecbusiness.co.uk

intecbusiness.co.uk

EXAMPLES OF CYBER SECURITY ATTACKS



Loss of reputation

A data breach through a ransomware attack or stealing of data and publishing on the internet, could have a serious impact on the reputation of the business. Once the compromise and breach have been published, the data and information has been released forever, there is no way of recovering or even knowing where the information will be published, it becomes public.



Loss of share value

A data breach, which impacts loss of reputation or even system downtime recovering from a ransomware attack or large-scale virus infection, if published could have a negative influence on share value and returns for investors. Some businesses will never recover from a major data breach or extended loss of systems.



Business interruption

Interruption due to a data breach can be costly, with the inability to function as a business, produce or sell goods, or even breach contractual obligations with clients.



Business continuity

Every organisation should have a Business Continuity Plan. It ensures everyone knows their responsibilities and actions, should major business interruption occur. It could involve restoring systems from backup, sourcing other cloud providers, but it should always involve disruption caused by Cyber Incidents.



Repeated blackmail requests from a data breach – double extortion

Unfortunately many businesses, once their data has been stolen by a hacker with blackmail demands to prevent publishing on the internet, repeated requests for money are being seen after the first payment. Once hackers have your data, there are no guarantees there aren't copies or it has in fact been sold to another fraudster.



Legal legislation

Many data breaches, whether insider, hacker or accidental, are in breach of UK data protection laws, GDPR or the Data Protection Act 2018, exposing the business to large fines from the Information Commissioner's Office. For example, both Marriot International and British Airways were fined around £20m each for data breaches of their client's personal information.

THE STATS DON'T LIE

The stats are compelling and speak for themselves. We're here to ensure that your business does not become the next victim of cyber attacks. So whether you would like us to review the security of your IT systems in general or you are interested in a specific element (e.g., remote worker device security, password protection, data backup...) get in touch to book your Cyber Security Audit.

REDUCE THE RISKS

As a Microsoft Gold Partner, we can offer helpful advice and implement the right solutions to protect the devices you use and the data you manage in your business every day. We'll ensure that the services you access are safe. We can also help you to stop unauthorised access to the vast amounts of confidential information you store on your device and online.

OUR CYBER SECURITY SOLUTIONS

CYBER SECURITY HEALTH CHECK

A cyber security health check will help you identify your organisation's weakest security areas. We'll recommend appropriate measures to mitigate your risk and conduct vulnerability scans of critical infrastructure LPS & website/URL.

CYBER ESSENTIALS AUDIT

Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks. Choose from Cyber Essentials or Cyber Essentials Plus, a certification which gives you peace of mind that your defences will protect against the vast majority of common cyber-attacks.

FULL SECURITY TESTING

Penetration testing, also called pen testing or ethical hacking, is the practise of testing a computer system, network or web application to find security vulnerabilities, that an attacker could exploit. Penetration tests assess your system for potential weaknesses that could result from poor or improper configuration, known and unknown hardware or software flaws. An experienced penetration tester will mimic the techniques used by criminals without causing damage, enabling you to address the security flaws that leave your organisation vulnerable.

BEST CYBER SECURITY OUTCOMES



Reduce the chances of security breaches



Maintain confidentiality of information



Minimise IT risks, possible damage and consequential costs



Increase trust with respect to partners, customers and the public



Obtain a competitive edge



Attract new business with the promise you have cyber security measure in place



Obtain a clear picture of your organisations cyber security



Follow a simple, straight forward process



Be listed on the directory of organisation's awarded certification



Increase your team's productivity

HOW CAN inTEC BUSINESS HELP WITH YOUR CYBER SECURITY AUDIT?

For complete peace of mind, protect your organisation's data, assets, and reputation with inTEC.

After contacting us, we'll be in touch as soon as possible to arrange an inTEC Security Audit. After completion, you'll receive a really useful report of your IT security capabilities and vulnerabilities along with a tailored list of recommendations of how you could improve your security. If you wish to move forward with any of the suggestions, we can make them happen.

Please contact us if you would like to discuss either continuing or starting your cyber security audit.



0345 565 1767

info@intecbusiness.co.uk

intecbusiness.co.uk