IS YOUR BUSINESS AT RISK?

Threats	Consequences	Causes
Cryptovirus A virus when downloaded holds your data ransom	• Loss of data (if no backups) • Loss of money (to pay the ransom) • Business downtime	• End User / Employees (Social engineering, lack of knowledge/awareness) • Insufficient email protection
 **Website Hacking/ Defacement** Attacker exploits vulnerabilities in your website to either remove or add content and uses it to deliver viruses to other people	• Brand reputation suffers • Your website gets blacklisted (i.e. Google, antivirus etc. might identify your website as a bad site to visit) • Loss of online customers	• Hosting provider compromised • Unsecured/outdated CMS • Application bugs 
Hacked Email Account Attacker successfully gains access to your email account	• Sends spam on your behalf, leading to your IP address getting blacklisted, blocking you from sending your own emails • Loss of custom & reputation • Loss of sensitive company & customer information	• Vulnerabilities in your servers, desktops or network devices • End User / Employees (Social engineering, lack of knowledge/ awareness) 
CEO Fraud Spoof email received enticing an employee to transfer money or perform other sensitive company actions e.g. change bank account numbers. – Usually seems like its coming from a trusted source, such as management, your lawyer etc.	• Large financial loss 	• End User / Employees (Social engineering, lack of knowledge /awareness)

www.Henocon.ie

Identify Risk

Penetration Testing

- Network
- Infrastructural
- Web Application
- Social Engineering

Mitigate

Infrastructure Hardening

- Firewalls, switches, routers
- Servers, desktops, thin clients
- Web applications, internet facing services
- Training

Prevent

Security Strategising

- Patch Management
- Disaster Recovery Planning
- Security Infrastructure Design

How do you protect your business and customers?

Most businesses have an online presence, leaving them at risk and vulnerable to attacks from malicious sources. While small to medium sized enterprises are most at risk, due to a lack of IT resources and knowledge, SMEs still have a responsibility to protect their own business not to mention their clients' data. SMEs are least serviced from an IT Security services perspective, as most IT Security providers assume a high level of IT support within their customers' organisation. This is where Henocon want to help you.

HENOCON are a dynamic provider of IT Security services. We specialise in security vulnerability identification and hacking attack methods in business IT systems. Through the use of these methods we can identify risk in your IT infrastructure and assist in mitigating against these – helping you ensure business continuity and brand sustainability.

Email: info@henocon.ie

www.Henocon.ie