Cybersecurity – Is this business' current greatest threat?

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from digital attack. In a computing context, security comprises cybersecurity and physical security – both are used by enterprises to protect against unauthorized access to data centres, computerized systems, and computing devices over the internet of things (IoT).

The most common cyber security incidents experienced are:

1. Ransomeware or Scareware– extortion through malware locking computers until payment is made.
2. Malware – malicious software created to be contracted so harm can be caused to data, software or hardware and includes:
    a. Viruses which attach themselves to clean files and infect other clean files
    b. Trojans which disguise themselves as legitimate software
    c. Spyware which hides in the background spying and gathering notes on what you do
    d. Worms which infect entire networks of devices either locally or across IoT
    e. Adware which is aggressive advertising software (really annoying)
3. Theft or breach of confidential information – theft of confidential information
4. Email phishing – attempts to trick you by sending hoax emails, getting you to click on dangerous links, or providing personal or financial information to an unauthorised source

Some statistics:

- During 2017 claims 516,380 Australian small businesses fell victim to cybercrime.
- 25 hours was the average downtime when attacked.
- $4,677 was the average ransomware demand for SME's
- $1.9 m was the average cost to medium to large business.
- ONE – the number of staff members that hackers need to dupe in order to gain access to your business' data!

In order to minimize the prospect of a cyber incident, you can:

1. Put one person in your business who is in management and has access to your data and assets in charge of cyber security – a Cyber Officer.
2. Get everyone in your business on board from bottom up.
3. Implement and maintain the latest anti-virus software.
4. Consult with an expert in cyber security in addition to your IT Officer or external IT provider.
5. Report, report, report – share each and every experience across everyone in your business, and with your customers.
6. Regularly audit your online footprint so you can identify and prioritise your risks.
7. Secure your systems, networks, (back ups, scans, sweeps etc)

8. Use complex passwords.
9. Consider cyber insurance.

For further advice on this topic please contact our team.

For more information contact our Intellectual Property Team.

Sam Davidson, Head of Intellectual Property

Ben Gouldson, Director

Simon Playford, Lawyer

Michelle Price, Paralegal

Nicola Hayden, Law Clerk

Contact Us

Phone 07 4688 2188

www.cglaw.com.au
