ICAEW

ICAEW Business Advice Service

Prepare for success

Top five cyber risks

Top five cyber risks

When setting up your new business, you are likely to rely on a variety of IT, such as smart devices, PCs and cloud-based systems. You could be holding customer data, employee information and possibly detailed product designs. These are likely to be of interest to cyber criminals – no matter how small your business. An awareness and basic understanding of the threats posed in a cyber-world will help protect your digital assets, intellectual property and your business.

There is a common misconception that small businesses are rarely a target for hackers because of their smaller size and lack of valuable data. However, any information stored on your systems might be interesting to criminals. Here are the current top five cyber threats that you should be aware of.

1. Ransomware

This is a form of malware (malicious software) that attempts to encrypt (scramble) your data and then extort a ransom to release an unlock code. Most ransomware is delivered via malicious emails. Follow these key steps to protect your company.

- Staff awareness: staff should be wary of unsolicited emails, particularly those that ask for a prompt response.
- Malware protection: install and maintain good anti-virus and malware protection software.
- Software updates: keep your applications up to date.
- Data backups: a series of well managed data backups will allow you to recover from an unencrypted version of a file. Make sure you regularly test your backups.

2. Phishing

Phishing is an attempt to gain sensitive information while posing as a trustworthy contact, for example a bank or online service. Spear phishing is a highly targeted attempt to gain information from an individual. Phishing emails may look completely convincing, often with faultless wording and genuine logos. There is a form of spear phishing, where a fake email from a CEO applies pressure on a CFO into making an urgent payment, this has become known as Whaling. It is worth considering ways to add additional safeguards to protect the identity of CEOs and CFOs to prevent impersonation. Here are a few steps you can use to protect yourself.

- Keep in mind that companies simply do not ask for sensitive information.
- Be suspicious of unexpected emails.
- Make use of anti-malware software.
- Make sure you have spam filters turned on. Check them regularly in case they have accidentally trapped an innocent email.

3. Data leakage

While cyber security in the office may seem challenging, it is essential to understand that security extends well beyond the office these days. The use of smart phones and tablets has become widespread. The ubiquitous and cheap nature of portable storage devices makes them a useful tool for the backup and transportation of data. Those features mean they are also a target for data thieves. The following pointers provide useful first steps to prevent data leaking from your organisation.

- Ensure mobile devices have passcode locks.
- Turn on the tracking by GPS and the option to remotely wipe the device if it is lost.
- The use of encryption software is highly recommended when using portable storage devices.
- Keep an eye on your mobile devices and paperwork at all times. A large proportion of crime is opportunistic, taking your eye off your briefcase or smart device could result in a serious loss of data.

4. Hacking

Gaining access to IT systems from outside an organisation still offers rich pickings for criminals. Traditionally they have attempted to gain access to bank account information or credit card databases. However, intellectual property is another source of value. The use of social engineering, tricking staff into revealing user names and passwords, remains a threat.

- The primary methods to protect yourself from hacking are network firewalls, data access security, procedures for providing and removing access, and user awareness and training.

5. Insider threat

If your organisation employs staff (full time or as contractors), there is a possibility they could leak data by mistake or maliciously. The potential damage from a leak of documents cannot be underestimated. Use these tips to mitigate the size of any data leak.

- Educate your team to be alert to issues and minimise careless mistakes.
- Limit how much data staff has access to. The principle of 'least privilege access' should apply to all IT systems. Only provide staff with the minimum access they need to do their roles.
- Control the use of portable storage devices, such as USB memory keys, portable hard drives and media players.
- Consider using applications in certain situations to monitor staff behaviour – who copies what.

In all these areas it is key to remember that alongside technology, well-developed processes, procedures and staff training go a long way to protecting your valuable data. For example, if someone leaves your employment, make sure you remove their access. The reality today is that you should protect your digital assets with the same vigilance as you do when locking your office door at the end of the day.

What to do if you have been breached

If the worst happens and you discover you have been breached, the following actions will help to contain the situation.

- Change your passwords, ensuring they are strong
- Call your bank and credit card companies
- Consider shutting your systems down
- Report the incident to ActionFraud
- Communicate to all involved, both external and internal. It is important all stakeholders, including customers and clients, understand what has happened.
- If appropriate, engage a third party expert to assess the extent of the breach and advise on corrective action.
- Document everything you do.

Consider creating an Incident Response Plan, outlining what you will do in the case of a breach – and ideally before you are compromised.

>> Useful sources of information

ICAEW Cyber Resource Centre
icaew.com/cyber

10 Steps to Cyber Security for Smaller Firms
icaew.com/10steps

Information Commissioners Office
ico.org.uk

Get Safe Online
Getsafeonline.org/businesses

ActionFraud
actionfraud.police.uk

If you need further help with getting to grips with cyber security, a free initial discussion with an ICAEW Chartered Accountant is a good place to start. Visit **businessadviceservice.com**

ICAEW Business
Advice Service

BAS

Prepare for business

Decisions you take in the early years of your business can be the most difficult as well as the most important, particularly if you are a first-time entrepreneur.

Prepare for success

The **ICAEW Business Advice Service** experts will help you make those crucial first steps and then grow your business with confidence.

Book a free consultation NOW
businessadviceservice.com

Prepare for business, prepare for success.

ICAEW Business Advice Service

The ICAEW Business Advice Service (BAS) provides professional advice for start-ups and owner-run businesses.

As well as practical help online in the form of white papers, short PDFs and blog articles, we enable businesses to receive an initial consultation at no charge from an ICAEW Chartered Accountant.

The **ICAEW IT Faculty** provides products and services to help its members make the best possible use of IT. It represents chartered accountants' IT-related interests and contributes to IT-related public affairs. It also helps those in business to keep up to date with IT issues and developments. As an independent body, the IT Faculty is able to take an objective view and get past the hype which often surrounds IT, leading and shaping debate, challenging common assumptions and clarifying arguments.

For more information on the IT Faculty visit **icaew.com/itfac**

Book a free consultation NOW
businessadviceservice.com

This leaflet is part of a series.
To find out about the others available visit businessadviceservice.com/guides