AUDIT • TAX • ADVISORY

10 steps to better cyber security

How to avoid a cyber-attack on your business

mha MACINTYRE HUDSON

An independent member of bakertilly INTERNATIONAL

Cyber security is never far from the headlines with companies large and small being victims of attacks.

The 2018 cyber attack on British Airways demonstrates that even a huge global business with IT budgets greater than the turnover of many businesses alone, were still unable to keep the hackers out.

As a business owner or non-technical Board Director responsible for IT, cyber security will be of great concern.

So how can you reduce the risk of a data breach in your organisation and avoid the heavy fines from the ICO?

We have set out ten key steps that you should review when considering your IT security.

1

Ensure you understand what data assets are important, applicable and relevant to your organisation:

- If you work in a regulated industry, ensure you comply with any applicable policies.
- Are there any sanctions that your organisation must adhere to?
- Do your customers demand that you comply with any recognised standards?

Has your organisation considered the impact of the GDPR (General Data Protection Regulation)? This applies to all organisations and, as a starting point, **you should:**

- Ensure you know where your data is and who has access to it,
- Conduct regular updates to your data policies and processes and ensure your employees comply with them, and review any measures you have in place to Prevent, Detect, and React to any breach.

2

Seek regular expert advice:

There is no shortage of articles on cyber security but unless you are in the security business then it can be difficult to understand the jargon and the areas that are applicable to your organisation.

- Consider outsourcing your IT. If it is already outsourced, then ensure your supplier provides proactive monitoring and keeps you updated on the latest threats.
- Ensure you subscribe to any security newsletters or updates from your security vendors (Firewalls, Antivirus vendors etc). Some cyber criminals will hunt for industry specific weaknesses. If your industry has an association or industry body, review any security advice they provide.

3

Identify your "Crown Jewels":

Each of your data assets will have a different value and it is not normally cost effective to provide the highest level of protection to all of them so you should therefore identify your "Crown Jewels" (any asset that requires additional protection) and apply elevated security measures to them. **For example:**

- Your customer databases,
- HR records and Payroll,
- Any Intellectual Property (IP),
- Company sensitive information, etc.

4

Keep your software up-to-date:

- Outdated applications and operating systems are vulnerable to security breaches. Ensure that they are kept up-to-date and patched regularly to avoid weak spots that hackers can exploit.
- Maintain software support agreements to provide access to the latest updates.
- Organisations that interact with customers through a website should ensure that the website is penetration tested annually buy a reputable security firm.

5

Ensure you have a robust password policy:

- A good password will have at least eight characters and contain a mixture of upper and lowercase plus special characters and numbers. Each additional character will greatly improve the strength of the password.
- Ensure that passwords on internal systems expire and cannot be reused.
- For assets that require additional protection, consider the use of two-factor authentication.

6

Educate your staff on the various phishing techniques:

Phishing is the most commonly used method for initiating a data breach. Hackers attempt to obtain sensitive information such as usernames and passwords by masking their identity in an email, which may appear to originate from a trustworthy organisation.

Some phishing emails may include attached documents which you should **NEVER** open.

- Most phishing emails will contain links to websites that may look legitimate but are indeed fake and will request that you enter sensitive information.
- A common technique is to use spoofed email addresses. These contain domain names that are very similar to yours, or ones you may be familiar with, but typically have a single letter that has been changed.

7

We have never had a security issue so why should we be concerned now?

- Cyber security is evolving all the time, as are the threats (and the fines from the ICO). It should not be something that you address once and then move on. It must be continually monitored and reviewed.
- You may think that your data has no value, but would you want your customer database to be available to your competitors, and what about your confidential employee data and payroll information?

8

Backup your data

- A data breach in a large organisation usually results in customer databases or intellectual property, being stolen. In smaller organisations however, the cyber criminals are not interested in your data, they are looking for financial reward.
- Viruses have been around for many years, but cyber criminals see Malware and Ransomware viruses as a lucrative money-making opportunity. Ransomware can sometimes be difficult to detect and may remain dormant for many weeks, but in the background they can be encrypting your data. Once finished it will display a message requesting you to pay a ransom before you can get your data back. You should never pay any ransom, even if it is your only option. Cyber criminals are not obliged to provide you with the key to unlock your data, so paying a ransom could only make the situation more painful.
- The only sure-fire way of restoring your data is from a recent backup. Backups should be taken at regular intervals, typically once a day, but certainly no less than the duration you can afford to lose. Ensure you keep your backups for several weeks before overwriting them and test them periodically to ensure they are functioning and backing up the correct data.
- All workstations and servers should have a reputable antivirus (AV) solution installed. This will often prevent a virus from causing too much damage, but these should be kept up-to-date. Some free AV solutions, and those built into the operating system, will detect many of the well-known viruses, but are typically not as good as those that you purchase.
- You can prevent many viruses from running by ensuring that your users are not logging into their PC's with admin privileges.

9

We might already be infected, is it too late?

So, if you have been infected by a virus or malware, it may be too late to recover the data from the local hard disk (unless you have a backup) so you should try and limit the damage and prevent the virus from spreading to other workstations.

The first things you should do are:

- Turn your computer off by the power button. Don't try and shut it down as you would do normally, it takes too long.
- Disconnect any cables that are plugged into it. These include power, network cables and any external devices.
- Ignore any ransom demands. It is unlikely they will unlock your data anyway.
- Call your IT helpdesk or support company for assistance.

10

Be prepared

- No organisation wants to experience a cyber security incident, but the reality is that most do at some point and without preparation, it could put your entire organisation at risk.
- You may be lucky and only experience isolated incidents, limited to one or two users with no residual loss of data however, this is no reason to become complacent.
- It is good practice to conduct a risk assessment and identify areas of your business that could be susceptible to a cyber security incident. Each risk should be scored based on the likelihood of the risk occurring and the impact it would cause to the organisation. This will set the priority in which the risks should be addressed. If you keep a risk log for other areas of your organisation, then these should be added to it and regularly reviewed.
- Larger organisations, or those that provide services to government or regulated businesses, may be required to comply with a recognised Information Security Management System (ISMS) such as ISO/IEC 27001:2013.
- Above all, be prepared.

MHA MacIntyre Hudson's Technology Advisory Services team has over 35 years of experience in helping organisations ensure that its IT systems and services are reliable, resilient, scalable and secure.

If you would like to discover how we could help your organisation, or you have any queries relating to this or any other IT matter, **please contact:**

Gavin Davis
Partner

T: +44 (0)1189 503 895
E: gavin.davis@mhllp.co.uk