Business Go Digital

HOW TO MAKE SURE YOUR BUSINESS IS NETWORK SECURE

Table of Contents

Introduction 3

It can happen to anyone 4

Home Wi-Fi routers 4

Uber 4

Yahoo 4

What are the implications of a network Security Breach? 5

Internal Measures: The first 3 steps 6

Security Audit 6

Backups 6

Educating Staff & Policies 6

Internal Systems & Equipment 7

Keeping Your Servers Safe 7

Keep your Software up-to-date 7

Secure Passwords 8

Storing passwords 8

Threat Prevention: Cyber Security 9

Anti-virus 9

Anti-ransomware 9

Spam filters 9

Remote Access Security 10

Limit access 10

Two factor authentications 10

Protecting External Data & Devices 11

Security 11

Encrypting Data 11

Backup Data 11

Legislation 12

GDPR 12

More information? 12

Introduction

You protect your business with locks and alarms as well as legally with insurance.

But many people consider network security as low priority or simply don't understand the risks and therefore ignore it.

Securing your business network is just as important as any other method of protecting your business.

Many businesses rely on the internet and if you are connected, you are at risk. And it doesn't matter what size your business is, cyber criminals don't target a business size, they search for vulnerabilities.

Almost half of all UK firms were hit by a cyber breach in 2017 (gov.uk)

There are many different types of network security breaches and they don't all occur online. This white paper will help you to better understand them, what the implications are, and show you ways to help keep your business network secure.

It can happen to anyone

We thought we'd start with some examples of both simple and high-profile examples of network security breaches that made the news. It just shows how many people and organisations are affected.

Home Wi-Fi routers

Last year, several models of Netgear home wi-fi routers were found to have a security vulnerability. This provided attackers with a way to compromise the associated network. Fortunately, once the threat had been discovered, Netgear quickly issued patches to address the issue.

Uber

The taxi firm suffered a data breach in 2016 with 57 million customers and drivers affected worldwide. Personal information such as name, address, drivers licence numbers and mobile phone numbers were leaked; the firm had to pay £75,000 for the data to be deleted to stop the information circulating.

Yahoo

Yahoo has been quite unlucky over the past few years. In 2016 they revealed that they were victims of two huge data breaches. Hackers stole extremely confidential information from their customer database. The breaches occurred in 2013 and 2014.

What is a network security breach? □ □ □ □ □ □

What is a network security breach?

A network security breach is an incident that allows unauthorised access to a computer network and its confidential data.

This could be performed by a malicious intruder or an automated application.

What are the implications of a network Security Breach?

Many businesses are not aware of the implications of suffering a network data breach, which ultimately affect the bottom line.

In 2017, 1 in 5 small businesses took a day or more to recover from their most disruptive breach (gov.uk).

When a network security breach occurs, the unauthorised users or automated applications can attack your business in many ways.

Here are some of the common motives behind why you might experience a security breach:

- **Theft:** Stealing sensitive or secure data.
- **Fraud:** Identity theft and financial information.
- **Destructive:** Deleting your data or stopping websites working.
- **Financial:** Encrypting your data for a ransom to be paid.
- **Competitive:** Theft of data, trade secrects, intellectual property.

These types of attacks could have major consequences on your business and not only financially, as the following examples highlight:

- **Lost revenue:** Your business may not be able to operate if your systems are not working or your data has been deleted.
- **Consumer Mistrust:** Customers may lose faith in your products, services or systems.
- **Damage to Reputation:** Suppliers and associates might re-consider their relationships with your business if your reputation suffers.
- **Financial Penalties:** Serious data breaches will incur fines from the ICO following the new GDPR legislation.

There are also many unseen or forgotten costs that can also be incurred after a network security breach.

- **Time:** Yours and your employees' time.
- **IT Costs:** The cost to detect and secure the breach and restore any backups.
- **Insurance:** Your insurance premiums may rise following a claim.
- **Notification:** You may need to notify any victims of the breach if you hold personal data.

There are products and services that exist to reduce these risks to businesses. In addition, they don't need the business owners to become experts in the field of network security.

Internal Measures: The first 3 steps

Security Audit

The first step is to perform a security audit. This is very important as it enables you to highlight any areas of your network that are vulnerable. The audit also needs to include mobile devices, home/remote workers' equipment and equipment taken out of the office, i.e. laptops and storage devices.

Backups

The second most important step is to ensure you have a comprehensive backup of all your data and you have tested the restore of this data. Network security is vital to your business, but if you have not backed up your data, you risk losing it.

Educating Staff & Policies

Educating your staff is paramount. Human error and social engineering (i.e. physiological manipulation by fraudsters) play a huge role in security breaches. Therefore, ensuring your employees stay vigilant and making them aware of common tactics that fraudsters use will help to reduce your risk. Also create a clear and simple security policy for staff to follow.

Internal Systems & Equipment

It is important to safeguard both the logical security (e.g. how people gain access to the systems across computer networks) and the physical security (e.g. how your building/server rooms are protected) of your systems.

Keeping Your Servers Safe

It's not just online security that is required to keep your data and files safe. Leaving your server in a room that is easily accessible can cause a lot of damage if it is broken in to.

You need to make sure that anything storing important and vital data is locked away safely and securely. If your server is onsite at your business' headquarters, keep it locked away in a separate room where it can only be accessed by authorised personnel. You will also need to consider the location of the sever room, for example regarding it's potential to be accessed by unauthorised personnel (e.g. room off a common area), or even flood risk.

If your server is stored offsite or in the cloud, you still need to take the same precautions.

Keep your Software up-to-date

Updates help to protect and keep your computer systems running smoothly. Outdated software, whether it's a Windows operating system or an application, can increase your risk of being attacked.

Hackers find it easier when a PC has outdated software which is a major reason why software companies provide regular updates. We advise that you check your PC and your applications for updates on a weekly basis if it does not automatically notify you.

Secure Passwords

Anything that holds confidential data, such as accounts packages, databases and spreadsheets, must be password protected.

You are more likely to suffer a data breach if you do not have password protection. This is something that everyone should be aware of.

Tips for strong passwords:

- Use a mixture of upper and lower-case letters
- Include special characters (e.g. #@>?!)
- Do NOT use your name, date of birth, or any other personal information
- Make your password 8 characters or more
- Do NOT use the same password for multiple accounts

Storing passwords

It can often be a struggle to remember all your passwords for all the different systems you use, especially when you are careful not to use the same password across different accounts!

Do not write down your passwords and do not share them with anybody.

A Password Manager stores all your passwords in a single secure account, keeping all your account details safe and secure.

LastPass is one such system. It securely stores all your passwords, and, once logged in, LastPass will automatically fill in your logon credentials for your registered systems and web sites.

Threat Prevention: Cyber Security

Measures need to be put in place to block potential threats from external sources. Here are some types of products you can use to protect your business:

Anti-virus

Anti-virus software helps to defend your PC's against malicious software.

There are many different types of computer viruses and new ones are regularly released. You can get basic products, often free of charge, or more sophisticated paid for packages with enhanced features. Many provide daily updates to address the latest known threats.

Anti-virus software is a must have, whether or not you have ever experienced having a virus on your systems; without this you may not necessarily know if you had!

Anti-ransomware

A virus and ransomware are two different things, so an anti-virus product may not necessarily prevent ransomware attacks.

Ransomware typically encrypts your files or locks your PC, literally holding your data to ransom. In such a situation we would advise not to pay, as this will encourage cybercrime.

You can protect yourself by using anti-ransomware and by using this in combination with anti-virus software, you can significantly reduce your exposure to this type of attack.

Spam filters

One of the ways viruses can get onto your computer is through phishing emails. They may be disguised as a legitimate company such as a bank, airline etc. and usually ask you to click on a link to verify details. By clicking on the link, you may inadvertently cause malicious software to be installed onto your PC, which may then permit unauthorised access to your PC and network and cause a serious data breach.

Spam Filters attempt to catch these malicious emails before they reach your inbox and provide you with the ability to delete those suspect messages before you download them.

Remote Access Security

Many businesses permit remote access into their systems, perhaps connecting servers to customers or supplier systems, or providing access to office systems for remote/home workers.

These connections can be potentially vulnerable to being intercepted for malicious purposes and need to be secured.

Limit access

Restrict access on a need to use basis rather than allowing wholesale access for all personnel. You could also restrict by hours of the day and days of the week where appropriate.

The fewer access routes into your systems the more difficult it is to exploit your remote access and the simpler it is to manage.

The way in which a hacker can gain access during your session is called a 'man-in-the-middle' attack. This means they intercept the session whilst you are active and can watch what is happening and listen in on the network traffic. This can be prevented by using authentication and tamper detection software.

VPN's

A Virtual Private Network (VPN) provides a safe and secure connection to allow staff to connect to the office or cloud server over the internet.

Consider a VPN for mobile staff who need to connect to your systems. VPN's offer a low-cost security option.

Two factor authentications

Two factor authentication provides an extra layer of security in addition to a username and password

For example, Apple use two factor authentication when a user logs into their account online. Before access is granted, a six-digit code is sent to the user's registered mobile phone, which must also be entered onto the site.

This method can also be implemented for secure access to a server, a document or PC. As hackers are finding more sophisticated ways of finding out usernames and passwords, this is a very useful way to add that extra layer of defence.

Protecting External Data & Devices

What many companies fail to recognise is that their data may leave the office or be stored externally. It can be taken out on laptops, storage devices or stored offsite on staff computers at home or in remote offices.

This data and the devices on which it is stored need to be protected.

Security

You need a security policy and cyber security software for your office, so you will also need the same for any remote workers or mobile devices taken out of the office. This also needs to be managed accordingly.

Encrypting Data

Encrypting data on offsite or mobile devices (e.g. laptops, usb drives, home workers computers) helps to secure your data should such equipment be stolen or mislaid; without the “key” the data is unreadable to an unauthorised 3rd party.

Backup Data

You may be backing up your data in the office, but any data that isn’t in the office should also be backed up. This can be sometimes difficult for some remote or mobile workers as their location or circumstances may prevent them from backing up data.

An excellent solution is to back up to the cloud as it provides an easy way to backup and recover files wherever you are.

Legislation

There are numerous pieces of legislation that are in place to help protect the confidential information of a business, their customers and employees.

GDPR

From the 25 May 2018, as many businesses are aware, the General Data Protection Regulation will come into effect, and is relevant to any business that processes data about individuals in the context of selling goods and services. This is to help strengthen data protection for everyone throughout the EU. It will supersede the current DPA (Data Protection Act 1998).

Its primary focus is to make sure that people are in control of their own personal data and to make sure that exploitation is dealt with efficiently.

Reference https:/www.eugdpr.org/gdpr-faqs.html

More information?

If you need more information or advice in what you can do to enhance your business' Network Security, please contact our helpdesk on 0777 842 9591 or email us at info@businessgodigital.uk

We can provide an onsite visit to meet with you and discuss your current security procedures and recommend what you can do to make your business compliant with Security and Data legislations.