



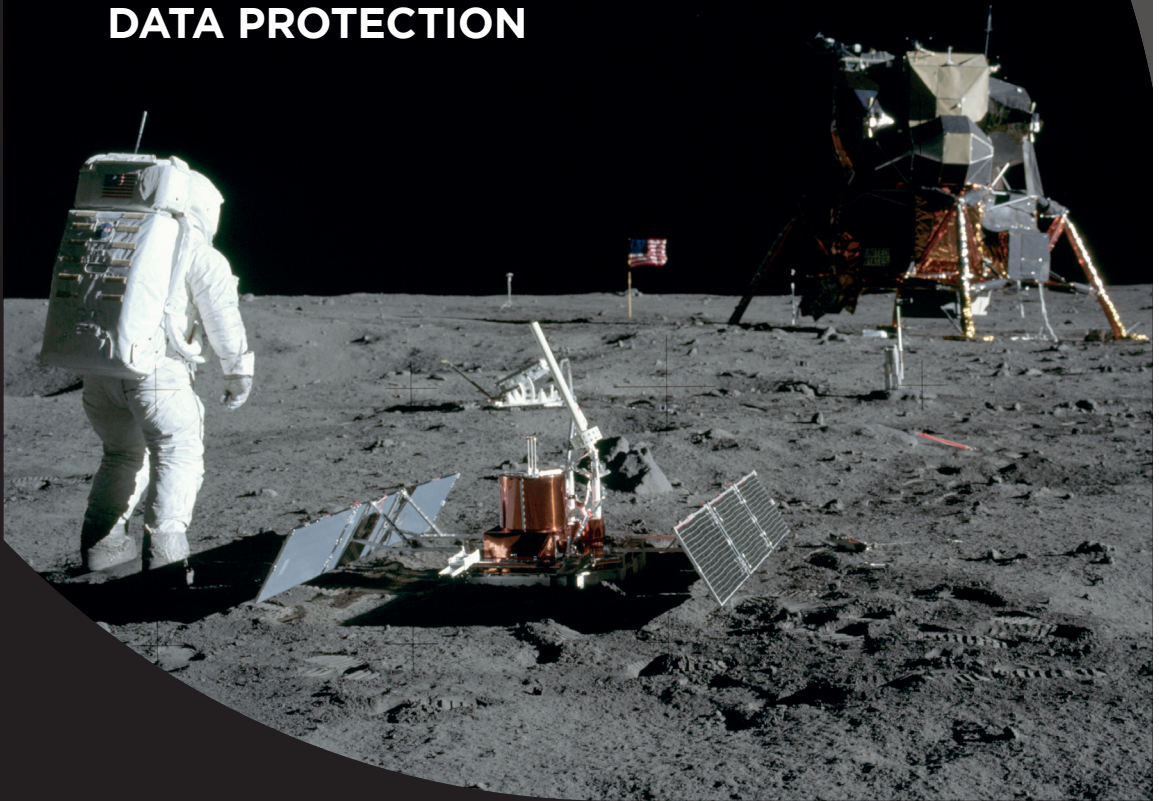
Herefordshire  
& Worcestershire  
Chamber of Commerce

PROTECTING YOUR DATA  
DOESN'T NEED TO BE A GIANT LEAP..

**JUST ONE SMALL STEP  
CAN GET YOU STARTED**

your guide to...

**DATA PROTECTION**



European Union  
European Regional  
Development Fund



WORCESTERSHIRE  
BUSINESS CENTRAL

# THIS GUIDE WAS COMPILED BY...

borwell 

 GOWLING WLG

Hallmark Hulme  
Solicitors

 Herefordshire  
& Worcestershire  
Chamber of Commerce

 TITANIA

SUTCLIFFE & CO.  
INSURANCE BROKERS



IASME Consortium<sup>®</sup>



NatWest

# CONTENTS

Foreword by Sharon Smith, CEO,  
Herefordshire & Worcestershire Chamber of Commerce .....4

Introduction by John Campion .....5

Why is data security important to my business? .....6

I don't need to protect my business... the misconceptions.....7

8 small steps you can take right now .....8

That was easy, what more can I do?..... 12

Need help or want to know more? ..... 13

What do some of these words mean? Easy access glossary. .... 14



**This guide will feature true stories from local businesses describing their experiences of cyber attacks.**



# FOREWORD



## SHARON SMITH

CEO, HEREFORDSHIRE  
& WORCESTERSHIRE  
CHAMBER OF  
COMMERCE

Businesses are becoming increasingly dependent on the internet to conduct their day to day operations. The rapid development of sophisticated digital connectivity can benefit productivity, efficiency and costs for businesses of all sizes and sectors. However, the internet is an inherently insecure environment, which can expose business operations to significant risks in the form of cyber attacks and threats.

As business becomes increasingly interconnected through networks, systems and devices, companies must address weaknesses in their cyber security to ensure operations are protected. It is vital

that businesses recognise that cyber security is a necessity not a luxury – just like the locks on their warehouses or the alarms on their offices. As businesses implement sophisticated online and digital systems, it is vital that they also keep pace with potential threats. By taking a number of small and often low-cost steps businesses can protect themselves from potential attacks.

Cyber Crime was identified by businesses in the two counties during 2019 as a key issue they would like the Chamber to address. To fulfil the objectives in the Chamber's 2019 Business Manifesto, we have collaborated with business leaders from across the two counties to put together this clear and concise guide. By outlining low-cost and simple preventative measures businesses can take, we intend to deliver on our promise to reduce the cost associated with doing business and facilitate greater connectivity in the business community across Herefordshire & Worcestershire.

# INTRODUCTION



“Technology and data have transformed the way we do business but we must all be aware of the huge risks and responsibilities this brings. However, with some basic know-how most threats can be easily eradicated or minimised with very little cost or effort. This guide will be a great help to organisations who want to create a culture of data security.”



**John Campion**  
**Police and Crime Commissioner**  
**West Mercia**

# WHY IS DATA SECURITY IMPORTANT TO MY BUSINESS?

Almost every business is now reliant upon data, electronic communication and electronic payments, and is connected globally by the internet and emails.

This brings great opportunities but also threats, as reliance and connectivity makes businesses vulnerable to accidental or malicious stoppages and breaches. In fact, the police now see more cyber enabled crimes than all other crimes put together<sup>1</sup>.

The General Data Protection Regulation (GDPR), introduced in 2018, has increased the responsibilities and penalties businesses face in relation to protecting personal data.

## 2 BIGGEST THREATS TO BUSINESS DATA SECURITY

### Human Error

The vast majority of data breaches are linked to human error<sup>2</sup>. This could be losing a laptop or briefcase, sending a confidential email to the wrong recipients or more commonly clicking on infected emails and websites.

### Criminal & Malicious Individuals

There are huge financial gains available to criminals if they can access your data or system. These include the copying and selling of your data, taking control of your data and extorting a ransom or stealing money by fraud or interception.

## BENEFITS DATA PROTECTION BRINGS TO YOUR BUSINESS

- **Protect your business, income, intellectual property and reputation**
- **Prevent interruption and disruption to your business**
- **Protect your customers and suppliers**
- **Avoid litigation and regulatory action**
- **Win contracts by demonstrating good standards of data protection and cyber hygiene with certifications like Cyber Essentials**

<sup>1</sup> Office of National Statistics (2018). [Online] Available at: [www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018](http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018)

<sup>2</sup> Ponemon.org (2019). [Online] Available at [https://www.ponemon.org/local/upload/file/The\\_Human\\_Factor\\_in\\_data\\_Protection\\_WP\\_FINAL.pdf](https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf)



# **I DON'T NEED TO PROTECT MY BUSINESS... THE MISCONCEPTIONS**

## **CYBER IS...**

### **...TOO COMPLEX, SO I WON'T UNDERSTAND IT**

Businesses already face many complex issues and risks regardless of their size. Treating the cyber risk just as you would any other risk can help mitigate the threat and, should the worst happen, help limit the damages to finances, down-time and reputation. The effective basics to prevent an attack can be straight forward (see page 8 for hints and tips).

### **...TOO SOPHISTICATED, SO I CAN'T DO ANYTHING ABOUT IT**

Many cyber-attacks can be prevented by having some simple, often free, measures in place; strong passwords are a classic example.

Nearly 50% of malware is delivered by email. By training your staff to look out for some simple 'warning signs', you and your team can keep your business resilient against online threats.

### **...NOT IMPORTANT, ATTACKS ARE TARGETED SO I'M NOT AT RISK**

Media stories regarding cyber security are often dominated by high profile attacks on large businesses or government departments. Many SMEs are often led to believe that smaller businesses are not targeted. In fact, the opposite is true. SME data is as valuable to criminals as large company data. Ransomware attacks are a common example.

Many attacks are general rather than targeted. Irrespective of company size or sector, the attack will be designed to target any company that has a particular weakness (vulnerability) in its IT systems. SMEs often display a number of vulnerabilities which become the focus of an attack.

Attackers target the weakest link in the supply chain. For example, one of your clients might be the target of an attack, but because their security is tight, the cyber-criminal will search for a weak link. Often the weak link is an SME supplier.

## 8 SMALL STEPS YOU CAN TAKE RIGHT NOW


### TRAIN YOUR TEAM

- There are plenty of free online resources that can help you and your team learn the basics. (See page 13 for some resources)
- Make sure the process for spotting and reporting suspicious activity is written up into formal policies and delivered consistently
- Recognise and encourage proactive behaviour through recognition awards
- To fully engage all colleagues, try testing their knowledge through fun games and mock phishing attacks

### BE VIGILANT WHEN PAYING SUPPLIERS

- Authenticate invoices for new suppliers and requests for changes in account details to prevent false payments
- For large payments transfer £1 and check it has arrived before paying the remainder of the invoice

### TRUE STORY



**A business suffered a 'ransomware' attack when an employee inadvertently opened a criminal's email and clicked on an infected attachment. This allowed the ransom virus to enter and entirely shut down the business' IT systems. As a last resort, the business paid the ransom but its data was still not returned and the business went into liquidation.**



## ENFORCE A SAFE PASSWORD POLICY

- Ensure employees use separate passwords for different accounts
- Passwords should be complex and secure
- Use three random words to come up with your password, this ensures it is secure and memorable
- Introduce upper and lower case letters, numbers and characters
- Computers, routers & firewalls often have default passwords which are widely known, change these straight away

## IMPLEMENT A 'BRING YOUR OWN DEVICE' POLICY (BYOD)

- Limit employees using personal phones & computers for work – you need control of the data and device security
- Restrict the use of USB sticks, disks and other devices that can transfer data and viruses

### TRUE STORY

**On checking their bank statement, a retailer found that for two weeks they had been sending out online orders to customers but the payments had not been received by their bank. On investigation they discovered their website had been hacked and all customer payments had been diverted to a criminal's bank account.**

## PROTECT ALL DEVICES WITH FIREWALLS & ANTI-VIRUS SOFTWARE

- Modern devices will often have firewalls or defensive software already installed. Ask about this when you purchase any new devices
- There are lots of reputable free versions of anti-virus software that you can install
- Remember if you do go for a free version of software, make sure you do your research before you install it, as you don't want to introduce new risks

## BACK UP YOUR MOST IMPORTANT DATA

- By backing up on at least a daily basis you can ensure that you will still have access to the data you need to operate your business if the worst happens
- Hold the back up data in a secure offsite location, or at least a fireproof safe onsite
- Make sure that the back up is tested to prove it works

## LIMIT ACCESS OF USERS AND UPDATE SIMPLE SETTINGS

Segregate your IT system so people only have access to the information that they need for their work. This helps to reduce risk of purposeful and accidental data breaches

Disable 'auto-run' on your PC. This feature automatically executes files without your input, including malware if it is present on your machine

Set up computers so they are in 'user' mode not 'administrator' mode, when used day to day. This will limit the ease of access if an attacker gets in

Set restrictions on standard 'users' so that they cannot install new programs without authorisation from an administrator (who can check they are safe)

## INSTALL UPDATES STRAIGHT AWAY

Often attacks will be automated to search for vulnerabilities which are known. Those who don't update are often caught out

Older software systems such as Windows XP are extremely vulnerable as updates are no longer released. Consider upgrading your operating system to one that is still supported

# THAT WAS EASY WHAT MORE CAN I DO?

DOESN'T SOUND TOO BAD?  
WHAT MORE COULD YOU DO?

- Aim to get certified to standards such as Cyber Essentials, IASME or ISO27001. These will give you security benchmarks to aim for and will reduce vulnerabilities
- Purchase insurance that will cover your cyber needs. This can assist you recover in the event of a data breach or cyber incident and cover costs and losses
- Consider getting an external vulnerability scan or penetration test of your business. This is where cyber security experts will try to find weaknesses in your system
- A route to your business may be through one of your suppliers. Check out the risk your suppliers pose and check what security measures or certifications they have in place



## TRUE STORY

**A business received a £17,000 email invoice for their new vehicle from their supplier. As everything looked correct they transferred the money. Unfortunately it went to a criminal bank account because the attackers had infiltrated the supplier's computer system and they were sending out fake invoices.**



## TRUE STORY

**A business employed an individual in their accounts department who, unknown to them, was part of a criminal gang. They installed malicious software onto the system which enabled them to syphon money and create fake invoices.**

## NEED HELP OR WANT TO KNOW MORE?

### NATIONAL CYBER SKILLS CENTRE

The government's main cyber security website. Comprehensive technical information and guidance.

**[www.ncsc.gov.uk](http://www.ncsc.gov.uk)**

### INFORMATION COMMISSIONER'S OFFICE

The government's website on data protection, especially GDPR. Lots of useful information that is user friendly. More focused on procedures than technical controls.

**[www.ico.org.uk](http://www.ico.org.uk)**

### GET SAFE ONLINE

General advice and tips on data security and cyber-crime. Lots of information, easy to understand. Also includes sections on social media and family.

**[www.getsafeonline.org](http://www.getsafeonline.org)**

### UK POLICE

Police website for reporting cyber crime.

**[www.actionfraud.police.uk](http://www.actionfraud.police.uk)**

### IASME

The local Accreditation Body for the Government backed Cyber Essentials certification scheme.

**[www.iasme.co.uk](http://www.iasme.co.uk)**

### RISK ASSESSMENT TOOL

Free vulnerability scanning software that will produce an easily understood report and instructions on how to rectify the finds.

**[www.titania.com/customers/bonus-tools/risk-assessment-tool](http://www.titania.com/customers/bonus-tools/risk-assessment-tool)**



# WHAT DO SOME OF THESE WORDS MEAN? EASY ACCESS GLOSSARY

## **Physical loss or theft of data or devices containing data**

A significant number of data breaches are as simple as losing documents, laptops or phones by either leaving them on public transport or in restaurants or having them stolen in a home or vehicle break-in.

## **User error**

User errors are common causes of data breaches and often occur when sending confidential emails to the wrong recipients by an auto fill address.

## **Phishing & Spear Phishing**

An email that is designed to lure the recipient into clicking on a link or opening an attachment. This will then either infect the user's system with a virus or encourage the user to reveal important information like bank account details. Phishing emails are normally quite basic and sent out in their thousands with the hope of catching an unwary user. Spear phishing emails are targeted at the individual recipient and are therefore more convincing.

## **Ransomware**

A virus that demands a ransom payment or you risk your data being deleted, locked or published. Often introduced from a Phishing email or infected website.

## **Denial of Service Attack**

The deliberate overloading of your system to prevent it working.

## **Spyware**

Malicious software that can enable a criminal to see everything on your system and even to take control of your system. They may even take over your hardware camera so they can see you too.

## **SQL Injection**

This occurs when a criminal gains access to the control of your website by entering control instructions into your website forms. This is especially serious if your website is transactional or connected to your business data.



### **Fake Invoices**

Criminals will send fake invoices and hope for payment. More sophisticated criminals will carry out research or use Phishing or Spyware to gather information so the invoice is convincing. They may even infect your business or a suppliers business so the invoice appears to be genuine or from someone within your own business.

### **Malicious behaviour by staff**

Disgruntled staff, staff leaving to work for a competitor or staff in receipt of bribes or blackmail can steal, copy or publish sensitive or valuable data, or install viruses. Data breaches can also occur due to the careless disposal of data or devices. Not only is it risky to throw sensitive documents in the bin, its important to be aware that old computers, printers, phones, etc. will have stored data on their hardware.

### **Vishing**

This is where criminals phone with the aim of tricking the recipient into revealing data or giving the criminal access to their computer system.



Herefordshire  
& Worcestershire  
Chamber of Commerce

**WORCESTERSHIRE  
OFFICE**

Severn House  
Prescott Drive  
Warndon Business Park  
Worcester  
WR4 9NE  
01905 673 600

**HEREFORDSHIRE  
OFFICE**

Skylon Court  
Coldnose Road  
Rotherwas  
Hereford  
HR2 6JS  
01432 803 236

goodbusiness@hwchamber.co.uk  
**www.hwchamber.co.uk**  
@hw\_chamber