Digital Scotland
Business Excellence Partnership

Cyber Resilience Toolkit

Making Scottish Business Cyber Resilient

Scottish Enterprise
HIE
Highlands and Islands Enterprise
Iomairt na Gàidhealtachd 's nan Eilean
COSLA
business gateway
your gateway to business expertise

Digital Scotland
Business Excellence Partnership

Contents

Welcome to the Cyber Resilience toolkit.

The following pages describe the problem facing small and medium sized businesses, introduce the security basics and benefits of becoming cyber resilient, and provide advice on questions to ask and where to go next.

Digital Scotland
Business Excellence Partnership

Introduction

A changing world

Technology has revolutionised small and medium sized businesses. It improves efficiency and is a channel to access a national and global base of customers. Technology enables us to share ideas and data and by using it well we can be faster, more responsive and more accessible.

The ideas, services and products that come from Scotland's SMEs are world leading. The information we create and the data we hold about our customers has value to us. It also has value to others. This makes us all a target of cyber crime.

The problem

Crime is increasingly moving online. Research has shown that SMEs are being targeted but they often underestimate their risk.

When businesses do understand the risk, they can find it difficult to get the right advice. There is a lot of advice available to businesses – but many struggle to understand which they should follow, what they should prioritise or where to go for help. This is where the toolkit comes in.

The toolkit

Cyber resilience can seem like a complicated topic and opinions differ on what to prioritise. You are uniquely positioned to help small and medium size businesses understand how to become more resilient.

This toolkit will:

- Provide you with a baseline knowledge of the cyber security landscape.
- Explain why businesses of all sizes are targets for organised criminals as well as opportunists.
- Explain the advantages of being cyber resilient.
- Provide basic advice to share with your clients.
- Signpost trusted sources of advice that clients can use to become more cyber resilient.

Digital Scotland
Business Excellence Partnership

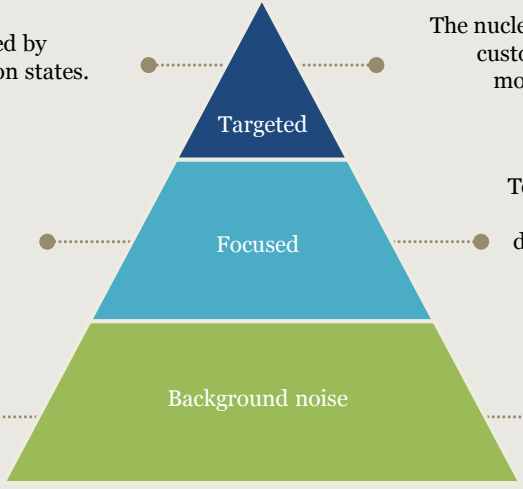
Cyber Landscape

A changing world

Hacking is a commercial enterprise. Large businesses are more likely to be attacked by nation states and professional criminal groups, whereas SMEs are more likely to be indiscriminately targeted.

Some organisations are directly targeted by competitors, organised crime and nation states.

The nuclear programme in Iran was sabotaged by custom malware. The 'Stuxnet' malware took months to develop and specifically targeted machinery used to process uranium.



Some companies are selected for their intellectual property or customer data. These attacks target every industry in the UK.[1]

Telecommunication companies are frequent targets because they hold lots of customer data. In Oct 2015, a teenager stole details of 157,000 customers from TalkTalk.

Hackers are opportunistic and search for soft targets. They use software to send millions of malicious emails, hack into websites and scan for unprotected internet connections.

Malware can be used to take control of computers. Groups of infected computers are known as 'botnets' and are used to attack websites and send spam. The 'Necurs' botnet controlled 6 million Windows computers and was shut down in June 2016.

The realistic approach

A motivated attacker with significant resources will eventually succeed. The good news is that SMEs are unlikely to be attacked by nation states and they can protect themselves against background noise and most focused hacking attempts. The simple suggestions in this booklet will stop more than 80%[2] of these attacks.

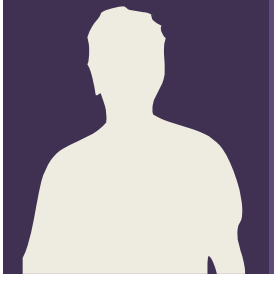
[1] NTT Security (*Global Intelligence Threat Report, 2014*)
[2] UK Government (*10 Steps to Cyber Security, 2012*)

Digital Scotland
Business Excellence Partnership

Mythbusters

The media reports on security breaches at large companies and movies dramatise cyber criminals. This leads to misconceptions about cyber security, as shown by the following security myths.

Being cyber resilient is too expensive.

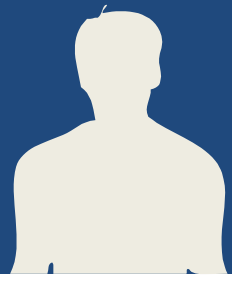


Getting the basics right goes a long way to making a business safe. The basics are often free or simply require changes in behaviour. Getting them right prevents disruption and lets owners focus on the main business.

There is no point trying to protect my business when the government and larger companies cannot protect themselves.

A motivated and resourced attacker can eventually breach any security system. Resilience is about finding a balance and having security that is proportionate to the risks faced by the business.

It is cheaper to fix problems when they occur rather than prepare for everything.



Security incidents are expensive. They impact reputation and revenue. There may also be fines for losing personal data. Good security wins business by showing customers you care.

My business is not a target because my data is not valuable.

Websites and any computer connected to the internet are targets. Hackers are opportunistic and use software to search for easy victims. Getting the basics right reduces the chance of being attacked.

I have a firewall and antivirus so my business is secure.

These are important but good security has many layers of defence. Behaviour and processes are just as important as technology.

Digital Scotland
Business Excellence Partnership

The Scottish SME Challenge

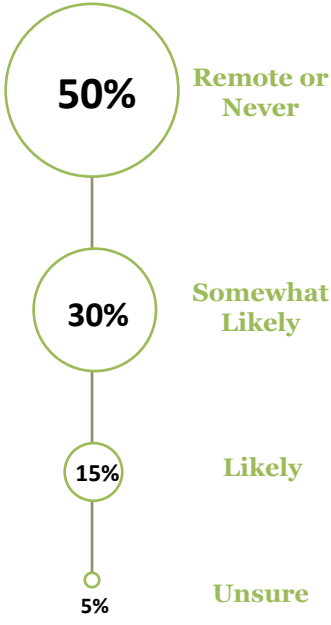
A recent survey conducted with small and medium sized businesses in Scotland by the University of Glasgow[1] shines light on some of the challenges faced when thinking about cyber resilience. The survey showed a clear desire for consistent and simple advice.

1. Companies struggle to know where to go for advice. There are too many sources of conflicting information.
2. Small businesses are concerned about security but many underestimate the level of risk they face.
3. Despite concern about security nearly 40% spend nothing on IT security and half are unsure they could detect an attack.
4. More than half of SMEs manage their own IT.
5. Most companies say information technology is very important to their business but that they are not worried about the security of their information.
6. Many companies recognise the need for basic controls to protect their business, but a quarter say controls such as antivirus and regular backups of data are unimportant.

[1] Karen Renaud (*Do SMEs care about Cyber Security, 2016*)

Question: Are you a target?

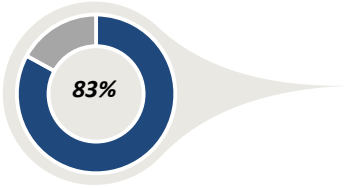
Scottish SMEs were asked their opinion on the likelihood of being hacked. Results support other research that suggests risk is underestimated.



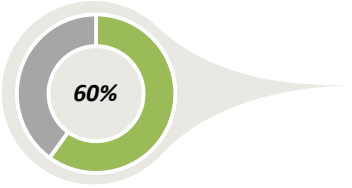
Digital Scotland
Business Excellence Partnership

In Numbers

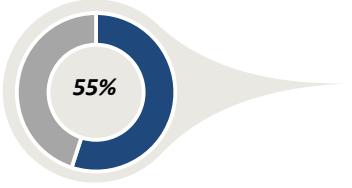
Small businesses are often reluctant to report security breaches but the following figures give an indication of the scale and nature of the problem in Scotland.



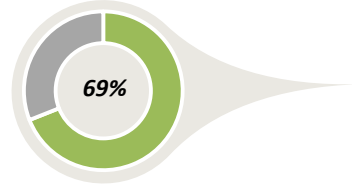
Consumers are concerned about how companies hold their data. In addition, 94% of procurement managers consider security when awarding contracts.[1]



The majority of small businesses had a security breach in the last year. The figure is much higher when data losses are included.[2]



Most people use the same passwords for their personal and business accounts.[3]



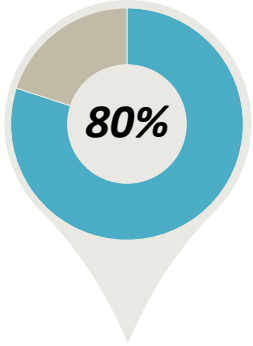
When businesses are compromised most find out later from a third party such as a supplier, customer or law enforcement.[4]

Cybercrime costs small businesses an average of **£3000** per year in remediation costs and lost business.

The most common types of cyber crime affecting small businesses are:

- Generic phishing emails (49%)
- Targeted phishing emails (37%)
- Malware attacks (29%)

Companies lose more than 2 days per breach.[5]



Basic security steps such as updating software will prevent over 80% of common attacks.[6]

1. Cyber Aware (*Small Business Reputation and the Cyber Risk, 2015)*
2. BIS (*Small Businesses: What you need to know about Cyber Security, 2015*)
3. Ofcom *(UK Adults Taking Online Security Risks, 2013)*
4. Mandiant (*M-Trends, 2015)*
5. FSB (*How to Protect Small Firms in the Digital Economy, 2016)*
6. UK Government (*10 Steps to Cyber Security, 2012)*

Digital Scotland
Business Excellence Partnership

Why Cyber Resilience

The Scottish Government has a vision[1] for Scotland being a world leader in cyber resilience. This is a future where we make the most of digital technology and manage the risks in order to create a global reputation for being a secure place to invest in business. Consumer confidence drives business growth.

Cyber resilience makes sense for Scotland but also locally for small businesses. Prevention is cost effective and being resilient is an opportunity to create value and differentiate a business from its competitors.

Value protection

Reduce risk and future costs

- Loss of reputation
- Costs to restore data and repair systems
- Restitution to customers and suppliers whose details have been stolen and used to commit fraud
- Data loss from computer infections or from failure to backup key business information
- Revenue loss from having designs and intellectual property stolen
- Fines from the Information Commissioner for failing to protect customer data

Value creation

Differentiate your business as a leader

- Enhance your reputation
- Show customers you take their information seriously
- Show suppliers you take confidentiality seriously
- Gain 'Cyber Essentials' certification and advertise commitment to best practice
- Bid for government contracts
- Take advantage of government funding schemes

[1] *'Safe, Secure and Prosperous: A cyber resilience strategy for Scotland' (2015)*

Digital Scotland
Business Excellence Partnership

The Cyber Resilience Journey

Cyber resilience is a journey and every business will be at a different stage of maturity.

The journey

Starting the journey

Risk and Response

Recognise that online crime is a risk to business. More than 60%[1] of SMEs had a security breach last year but 65%[2] still think they are not a target and nearly 40%[2] spend nothing on security. The media report breaches at large companies and this contributes to a false sense of security among small businesses. Think of cyber security like physical security: passwords are locks, firewalls are fences, anti malware is the alarm system and backing up data is contents insurance.

Becoming cyber resilient

Sensible Security

Small businesses do not need the same security system as a bank because the threats are not the same. Security is about understanding the risk to the business and taking the proportionate steps. For many small businesses this can be achieved using free or low cost tools, educating employees and applying Cyber Essentials. Preventing attacks is one part of resilience, the other part is being able to recover from attacks with minimal disruption to the business.

Staying cyber resilient

Good Behaviour

Cyber resilience is about behaviour and not just technical defences. Educating employees about good practice regarding passwords, backing up data and keeping software up to date are equally important. As a business grows the threats it faces will change. It is important to regularly review security practices and to inform employees of change.

[1] BIS (*Small Businesses: What you need to know about Cyber Security, 2015*)
[2] Karen Renaud (*Do SMEs care about Cyber Security, 2016*)

Digital Scotland
Business Excellence Partnership

Cyber Essentials

Cyber Essentials is about helping businesses get the basics of security right. The government scheme was introduced in 2014 and simplifies security requirements into five key steps. Certification is required to bid for government contracts.

The Essentials form a key line of defence against cyber crime. Additional detail on the tools mentioned here can be found in the Easy Wins glossary at the end of this document.

1

Boundary controls

Protect the online doors and windows of the business. Firewalls prevent unauthorised access from the internet and are an important control. Password protect Wi-Fi and avoid using public Wi-Fi to conduct business.

2

Secure configuration

Using applications as they come 'out of the box' can be unsafe. Secure configuration is about limiting opportunities for attackers. Disable unused accounts and services. Use strong passwords and backup your data regularly.

3

Access control

Restrict access to valuable data and systems. Make sure accounts are cancelled when employees leave the company. Log out from computers when stepping away, and monitor accounts with special permissions such as administrator accounts.

4

Anti malware

Anti malware scans computers looking for malicious files and program behaviour. Make sure anti malware is installed and set to automatically check for updates to protect against new threats.

5

Patching

Hackers target old and vulnerable systems. Stay safe by keeping systems up to date. This can involve ensuring automatic updates are enabled and updating web browsers. Delete programs that are not required for work.

Digital Scotland
Business Excellence Partnership

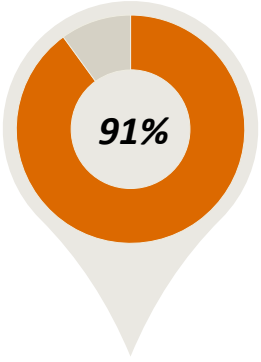
Your First and Last Line of Defence

Cyber Essentials helps businesses implement technical defences against cybercrime. Security though is not just a technical challenge, it is about changing behaviour. Employee education is your first and last line of defence.

Employee education

Are you confident staff will recognise suspicious emails? Do they open links and attachments only if they recognise the sender? Will they change customer and supplier details only if the request comes from existing contact details?

Employee education should extend to cover the importance of having strong passwords and making sure that devices holding data are password protected. It should also include basic security measures such as locking computer screens when leaving desks and the risks of conducting business over public Wi-Fi.



It is estimated that 91%[1] of targeted cyber attacks begin with a phishing email. On average 23% of users open phishing emails and 11% open attachments[2].

Phishing

Hacking can be hard work. It is much easier to send emails and trick employees into clicking links or opening attachments. This is known as phishing.

Spotting the danger

Phishing emails have many common danger signs:

Urgent	You need to pay an invoice, update a password or claim a prize.
Sir/Madam	The email does not know your name.
Please click	You are asked visit a website or open an attachment.
Spell check	The email may contain spelling mistakes and poor grammar.
Imitation	The email address is similar to a real company but has extra characters.
Misdirection	When you hover your mouse above the link it shows a different website address.

Ransomware

Malware that locks the files on a computer and demands a ransom is increasingly common. It is important to regularly backup data to reduce this threat. Paying criminals is risky and there is no guarantee they will unlock files.

[1] Trend Micro (*Spear-Phishing Email: Most Favored APT Attack Bait, 2012*)
[2] Verizon (*Data Breach Investigations Report, 2015*)

Digital Scotland
Business Excellence Partnership

Where to go for Help

There are many good sources of information online if you know where to look.

Organisations are listed here which offer practical advice and support.

Cyber Essentials is a government backed scheme to help businesses understand and get the basics right. Certification is obtained by completing a questionnaire that is evaluated for a small fee. This provides a basic level of assurance and allows bidding for government contracts.

https://www.cyberaware.gov.uk/cyberessentials

National Cyber Security Centre- UK Government dedicated centre that provides advice for businesses and individuals on adopting secure online behaviours to protect their data and devices.

https://www.ncsc.gov.uk

Get Safe Online provides accessible advice to keep businesses and individuals safe online. They provide a wide range of advice on protecting your computer and smartphone, buying and selling online, and on avoiding common scams.

https://www.getsafeonline.org

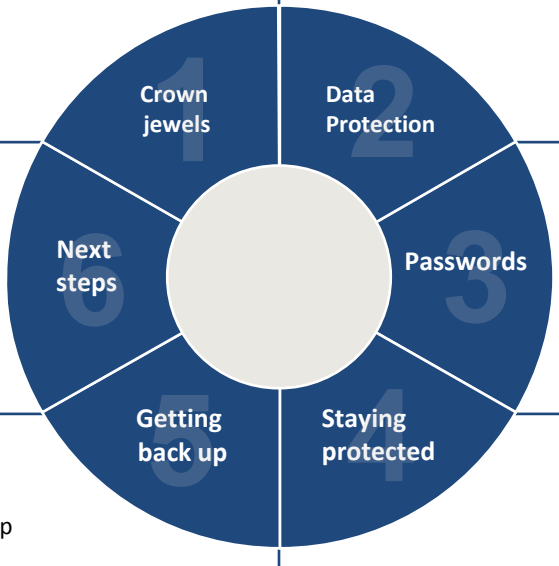
Cyber crime often goes unreported. This can mean that the right resources are not directed at fixing these problems. If the worst happens to your organisation it is important that you contact **Police Scotland** on **101**.

If you have any queries about further support available please discuss this with your local Business Gateway, Scottish Enterprise or Highlands and Islands Enterprise contact.

Digital Scotland
Business Excellence Partnership

Accelerators

This slide outlines some conversation accelerators aimed at helping you have a productive conversation about cyber resilience.



- What is your most important data?
- How do you protect this information?
- Where is your data stored?
- Who has access?

- Do contracts with third parties say who protects your data?
- Are employees trained to password protect removable storage devices?
- Have you ever reviewed user accounts to make sure employees have appropriate access?

- What is your plan for educating employees about security?
- Have you considered becoming Cyber Essentials certified?
- Did you know Scottish Enterprise and HIE have dedicated IT advisors?

- Are passwords for all personal and business accounts the same?
- Do you use a weak password that is short or one that can be found in a dictionary?
- When is the last time you changed your passwords?

- When is the last time you backed up your most important data?
- Have you checked that your backup copies actually work?
- How would you respond if an attack deleted the files on your computers?
- Who is responsible for keeping copies of your website?

- Are you using the latest version of your internet browser?
- Do you use software that is no longer vendor supported?
- Does your anti malware update automatically and scan regularly?

Digital Scotland
Business Excellence Partnership

Easy Win Glossary

Term	*Description*
Antivirus / Anti Malware	Anti malware software scans computers for malicious programs. A 'dictionary' is used to recognize suspicious files which are then deleted. There are many free antivirus programs. A good program lets you schedule scans and will automatically download new definitions when the dictionary is updated.
Firewall	Firewalls prevent access to computers from the internet. They also enable you to block employee access to dangerous websites. There are many free firewall programs. Most computers already have one because both the Windows and Apple operating systems come with firewall applications, which by default are turned off.
Patching	Criminals target old software because these have known vulnerabilities. Internet browsers are commonly attacked and so are constantly updated to stop these attacks. You can visit WhatBrowser.org to check if you have the latest version and upgrade for free.
Backup	Copy important business information regularly and keep copies in a separate and secure location. The more important the data, the longer copies should be retained before overwriting them. Remember to occasionally check that backup copies work.
Passwords	Passwords control electronic access the same way locks control physical access. Longer is stronger, and GCHQ recommends using three joined words. Make sure business accounts use different passwords than personal accounts. Changing passwords periodically protects accounts from existing intruders and from insiders who wish to steal data.
Wi-Fi	Data sent using Wi-Fi can easily be intercepted. Password protect the office Wi-Fi and avoid conducting business over public Wi-Fi unless you trust the connection. Always manually select available Wi-Fi networks rather than letting your smartphone automatically connect.
Privileged Accounts	Administrator accounts need to be carefully controlled because users can change everything the system allows. These privileged accounts should be restricted to appropriate employees. Passwords should be periodically changed and never shared between employees.
Third Parties	Businesses are increasingly using third parties to host and manage data. Contracts should state who is responsible for backing up and protecting data. Make sure that data stored on free services will not be lost if the service becomes unavailable.

Notes


Digital
Scotland
Business Excellence Partnership