DIGITAL BOOST

power up your business

CYBER RESILIENCE GUIDE

Digital Scotland

business gateway

your gateway to business expertise

TABLE OF CONTENTS

SECTION 1
WHAT IS CYBER RESILIENCE?

Cyber resilience is the process of how a business responds to cyber threats. In today's modern landscape, businesses not only need to defend from attacks – they must also plan responses to successful security breaches.

CYBER SECURITY VS CYBER RESILIENCE

Cyber security primarily focuses on a business's capability to defend itself against cyber-attacks. Cyber resilience has a wider focus, encompassing security but also business resilience – adopting a culture of awareness and an ability to recover from cyber-attacks.

A good cyber resilience strategy must focus on:

- ✔ Prevention
- ✔ Risk management
- ✔ Response
- ✔ Recovery

All businesses should adopt preventative measures, as sometimes prevention is better than the cure. In 2016 RiseArt, an online art store, were able to reroute malicious traffic from a cyber attack. By being vigilant and practicing proactive techniques, they were able to keep their services online.

Practicing the basic steps can prevent most cyber-attacks. Being able to then identify and respond to successful security breaches are critical for business resilience.

SECTION 2

WHY CYBER RESILIENCE IS IMPORTANT?

Despite 93% of small firms taking steps to protect their business from digital threats, 66% have been a victim of cyber crime in the past two years. During that period, on average those affected have been victims on four occasions – costing each business almost £3000 in total. [Federation of Small Business]

Failing to take basic steps can result in fines too. In 2014 Boomerang Video had the details of over 26,000 customers stolen. The Information Commissioner's Office (ICO) found they had failed to take basic preventative measures, and fined the company £60,000.

I'M TOO SMALL TO BE ATTACKED

This is a common misconception, in the last 12 months 38% of micro firms (2-9 employees) experienced a cyber security breach or attack. [UK Government Cyber Security Breaches Survey: April 2017]

OUTCOMES OF CYBER BREACHES

In 2015 a Scottish hairdressing business was hacked, which resulted in a loss of all their appointment data. While you might think your business has nothing worth stealing, cyber breaches can cause damage in other ways:

- Temporary loss of access to files or networks
- Software or systems corrupted or damaged
- Website or online services taken down or slowed
- Permanent loss of files

- Money stolen
- Personal data altered, destroyed or taken
- Theft of intellectual property

THE IMPACT

The impact of such breaches can have more than a simple financial impact:

- Business unable to function commercially
- Loss of competitive advantage
- Loss of reputation
- Loss of intellectual property

SECTION 3

BASICS OF CYBER SECURITY

To provide a foundation of basic measures that all organisations can build upon, the Government and cyber security industry have developed the Cyber Essentials scheme. It has two primary functions:

- Provide a clear statement of the basic controls organisations should implement to mitigate the risk from common internet based threats
- Allows organisations to demonstrate they have taken these essential precautions to customers, investors, insurers and others

The Cyber Essentials scheme has been designed in consultation with Small and Medium sized Enterprises (SMEs) to be light-touch and achievable at low cost. While significantly reducing an organisation's vulnerability, it is not designed to address more advanced, targeted attacks.

Similar to any other business risks, organisations should assess the threat they face and implement additional measures as part of their security strategy.

Cyber Essentials five key controls:

- **Boundary firewalls and internet gateways** - these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.
- **Secure configuration** – ensuring that systems are configured in the most secure way for the needs of the organisation.

- Access control – Ensuring only those who should have access to systems, have access and at the appropriate level.
- Malware protection – ensuring that virus and malware protection is installed and is it up to date.
- Patch management – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor have been applied.

SECTION 4
BOUNDARY CONTROLS

Computers can communicate using over 65,000 different possible channels called “Ports”. If a port is left open, it can allow someone else to ask your computer to do something malicious.

FIREWALLS

Firewalls are an important control that help stop attacks on your systems. They act like traffic lights:

- Red – do not communicate
- Amber – communication filtered and restricted
- Green – communicate

WHAT CAN I DO?

✓ Ensure all devices and networks are protected, and switch the firewall on

✓ Configure the firewall to allow only necessary communication, close down ports except those known and used

✓ Control your firewall with a password

SECTION 5

SECURE CONFIGURATION

Computers and network devices may not always be secure in their default configurations. Weak points in standard 'out of the box' configurations may include:

- An admin account with a pre-set, publicly known default password
- Pre-installed but unnecessary applications and services
- Pre-installed user accounts with special access settings

Secure configuration is focused on limiting opportunities to attackers.

WHAT CAN I DO?

✓ Create an audit of systems your business uses

✓ Decide who needs access to what systems, and limit access strictly to the user need

✓ Use strong passwords

✓ Disable unused accounts and services

✓ Backup your data

SECTION 6
ACCESS CONTROL

Within your organisation, every active user account facilitates access to devices and applications. Special privilege accounts have even more access, an exploited account could result in large-scale corruption of data and disruption to business processes.

You must understand who has access to your data, and ensure the appropriate restrictions are in place for valuable assets and systems.

WHAT CAN I DO?

- ✓ Restrict access to valuable data and systems
- ✓ Regularly check who has access
- ✓ Give thorough checks on 'privileged' accounts that have more access than others

SECTION 7
ANTI-MALWARE

Downloading software from the internet can expose a device to malware – such as computer viruses, worms and spyware. Sources of malware include email attachments, downloads and installation of unauthorised software.

Anti-malware scans your files, system and email, searching for malicious content or behaviour. If a system is infected with malware, your organisation could experience malfunctioning systems or data loss.

WHAT CAN I DO?

- ✓ Deploy antivirus and malicious code checking solutions to continuously scan inbound and outbound objects
- ✓ Deploy a content filtering capability on all external gateways, which will try to prevent malicious code being delivered to desktop applications
- ✓ Only use software known to be trustworthy
- ✓ Where possible disable auto run functionality, which should prevent the automatic import of malicious code
- ✓ Scan every network component on a regular basis
- ✓ Ensure all anti-malware software is kept up to date

SECTION 8
PATCHING

Keeping systems up to date is essential, as hackers target older or vulnerable systems. Patch management is the process of managing system and software updates – including how and when they are kept updated, change control and testing.

The WannaCry attack on the NHS in 2017 was due to vulnerabilities in computers that had not applied a recent patch update from Microsoft.

Once exploited, software was installed which encrypted all user files and demanded payment for them to be unlocked.

WHAT CAN I DO?

- ✓ Patch known vulnerabilities with the latest version of the software
- ✓ Ensure the latest supported version of an application is used

SECTION 9

TRAINING STAFF AND DEALING WITH THIRD PARTIES

Maintaining awareness of cyber risks within your organisation ensures staff become a cyber asset. They will become less susceptible to vulnerabilities, and be better able to detect malicious behaviour – acting as the first line of defence for your organisation.

YOUR STAFF SHOULD:

- ✓ Be aware of good practice regarding passwords
- ✓ Back up data regularly
- ✓ Keep software up to date
- ✓ Lock computer screens when away from desks
- ✓ Realise the risk of conducting business on public Wi-Fi
- ✓ Understand and follow the organisation's cyber security polices
- ✓ Educating staff should be an ongoing process as the cyber landscape shifts

INCIDENT MANAGEMENT TEAM

When a cyber breach has been detected the pressure will be on. It is critical incident response roles are assigned to staff beforehand to ensure a swift response.

YOUR RESPONSE TEAM:

- ✓ Must possess the skills and knowledge required to respond to an incident
- ✓ Have a team leader that determines when an incident has occurred

- ✔ Should follow a clear procedure, using clear communication and coordination
- ✔ Should ensure compliance with existing procedures

If weaknesses are found within then action must be taken. In 2016, vulnerabilities were found in Tesco Bank's mobile app. Despite being made aware of these issues, the company hadn't taken immediate action.

Eventually the vulnerabilities were exploited by hackers who stole £2.5 million in customer money. While the bank reimbursed customers – the revelation Tesco Bank had not acted on known vulnerabilities was just as damaging for consumer trust.

SECTION 10
RECOVERY

In the event of a successful cyber breach, a recovery plan is essential for your organisation to be resilient.

HAVE A PLAN

- Planning is critical to determine crisis-management and incident-management roles
- Arrangements should be made for alternate communication channels, services and facilities
- Explore different "what if" scenarios to identify gaps in your organisation before an incident occurs
- Exercise technical and non-technical aspects of recovery, such as personnel considerations or facility issues

Recovery planning is fluid and not a one-time activity. You should continually review and improve upon your procedures. This can be achieved through lessons learnt, and periodically validating the recovery capabilities themselves.

Use metrics to measure the effectiveness of the recovery process, and determine if it was a success.

BUILD A RECOVERY PLAYBOOK

- Develop an inventory of all important information assets
- Identify what has been impacted by the incident and check against inventory
- Try to store configuration information to assist recovery
- Ensure where possible there are backups
- Keep everything maintained and up to date
- Measure and track the performance of the protective steps taken

SECTION 11

OTHER RESOURCES/ FURTHER READING

- ISO27000 Family of 19 Cyber Security Standards
  https://www.iso.org/isoiec-27001-information-security.html
- ISO22316:2017 Organisational Security and Resilience
  https://www.iso.org/standard/50053.html
- DigitalBoost Cyber Resilience Online Tutorial
  https://www.bgateway.com/online-tutorials
- Cyber Essentials
  https://www.cyberaware.gov.uk/cyberessentials/
- CiSP (Cybersecurity Information Sharing Partnership
  https://www.ncsc.gov.uk/cisp
- Get Safe Online (Business)
  https://www.getsafeonline.org/business/
- NCSC Cyber Risk Management
  https://www.ncsc.gov.uk/topics/risk-management
- The Information Commissioner's Office (The ICO)
  https://ico.org.uk

CONTACT YOUR LOCAL BUSINESS GATEWAY OFFICE

Get expert advice on this and a wide range of topics for free at your local Business Gateway office.

bgateway.com/local-offices