SMALL BUSINESS CYBER SECURITY TOOLKIT

EVERY GREAT JOURNEY STARTS WITH THE FIRST STEP

SWCSC
SouthWest Cyber Security Cluster

CYBER SECURITY IS ESSENTIAL FOR THE SECURITY OF YOUR BUSINESS

Of small businesses had an information security breach in the past year - source: www.gov.uk

is the average cost to a small business. (Up from £35k a year ago) - source: www.gov.uk

of small businesses close within 6 months of a major cyber attack - source: smallbiztrends.com

You can protect your business against this crime

SWCSC
SouthWest Cyber Security Cluster

ABOUT SWCSC

The SWCSC is a not for profit collaboration supported by the police, leading universities, industry experts and business organisations. The Cluster exists to raise the profile of cyber security issues and help the region's businesses and organisations take steps to counter the threats. For further information please visit https://southwestcsc.org/

SWCSC
SouthWest Cyber Security Cluster

WHAT'S THE PURPOSE OF THIS TOOLKIT?

This guide has been set up to provide clear and simple ways to keep your organisation safe in the online world.

Developed by Cyber Professionals in the South West, it provides you with the simple, first steps you need to make your business cyber resilient.

The toolkit provides guidance and content to help you on an easy journey to build your policies, process, and procedures to develop a compliant and safe organisation.

Disclaimer: All information has been developed in good faith, the Cluster nor any members can be held responsible for any actions or incidents as a result of utilising the content or links on this toolkit. If any links are no longer valid, please email us info@southwestcsc.org

SWCSC
SouthWest Cyber Security Cluster

5 STEPS TO CYBER SAFETY

SWCSC
SouthWest Cyber Security Cluster

IDENTIFY

Identify how much cyber risk you have in your organisation

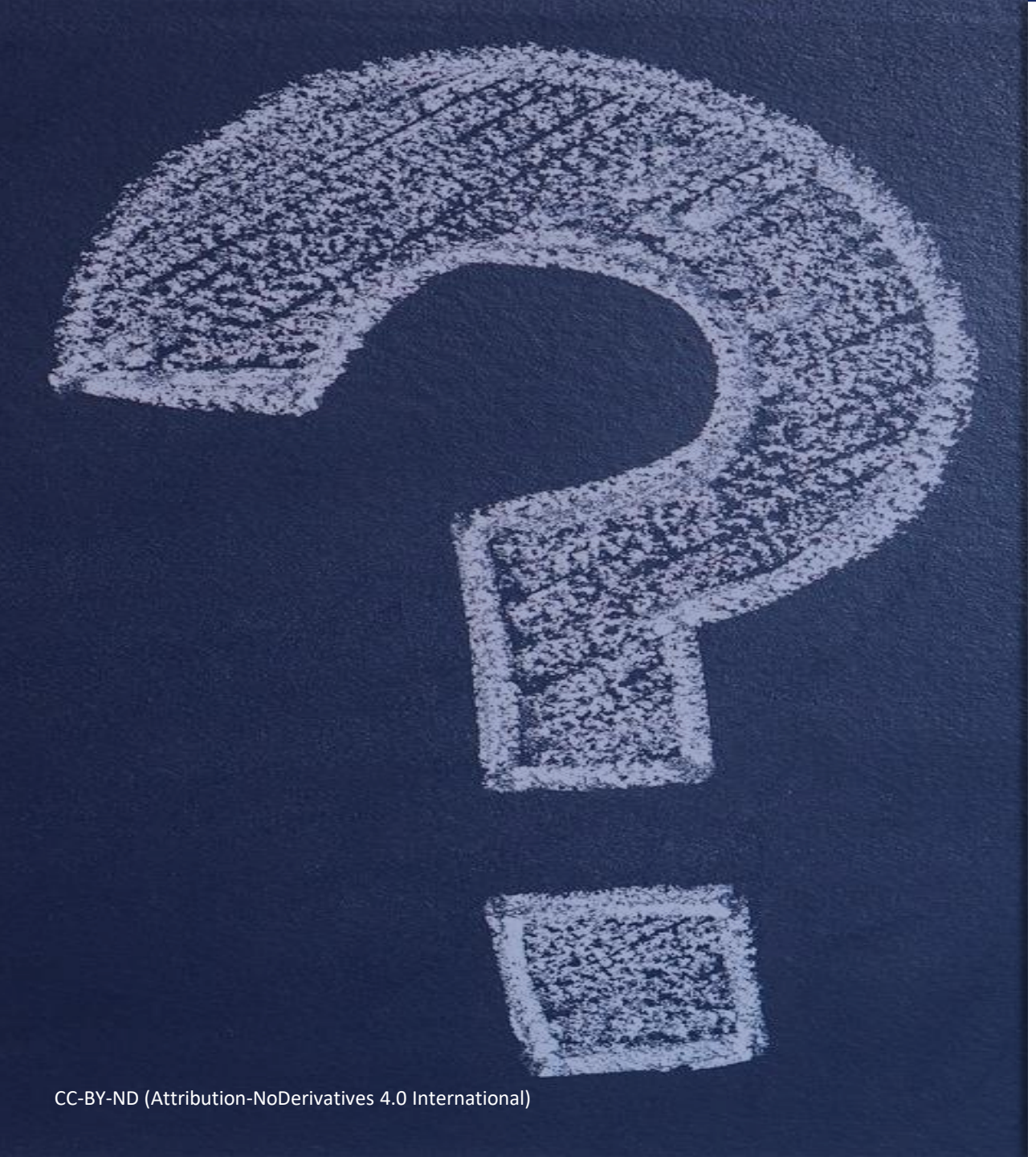
SWCSC
SouthWest Cyber Security Cluster

Introduction to identify

Identify is the first of the ‘five steps’ and it calls for companies to develop a better understanding of the risks which could affect their ability to operate.

We are all busy in our day to day activities but taking out some time to understand what assets we have, which are important or critical to our operation and how we can reduce our risk is imperative in today’s connected world.

SWCSC
SouthWest Cyber Security Cluster



KEY QUESTIONS:

- What digital assets have you got?
- Where does it live?
- Who's responsible for it?
- What's my risk?
- What should worry me?

SWCSC
SouthWest Cyber Security Cluster

ASSET REGISTER TOOL

What is an asset register?

An Asset Register Template is a list of your:

- Hardware
- Users
- Software
- Locations
- Cloud Services

It can provide a view of your important data that might be classified as:

- Business Confidential
- Personal
- Sensitive
- Regulated

Download an asset register template here

SWCSC SouthWest Cyber Security Cluster

RISK MANAGEMENT QUESTIONS

How does a cyber incident affect my disaster recovery plan?

https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics

Here's a quick quiz to identify your fraud awareness

https://www.barclays.co.uk/digisafe/digitally-safe-quiz/

SWCSC
SouthWest Cyber Security Cluster

RISK MANAGEMENT QUESTIONS

Can my business continue if….

- My data is locked?
- I'm held to ransom?
- I can't talk to my customers?
- I don't have email?
- If my website is hacked?
- My staff can't work as my systems aren't available?

SWCSC
SouthWest Cyber Security Cluster

RISK ASSESSMENT ESSENTIALS

"Capture and assess the cyber risks in the context of my business "

Download the Risk Assessment template here

SWCSC
SouthWest Cyber Security Cluster

COMPLIANCE REQUIREMENTS

What else?

What are the requirements for my business to stay legal and compliant?

Legal requirements
GDPR - Data Protection Act
E-Privacy
PCI Compliance

Supply Chain requirements
Cyber Essentials

Cyber Insurance - Is it right for you?

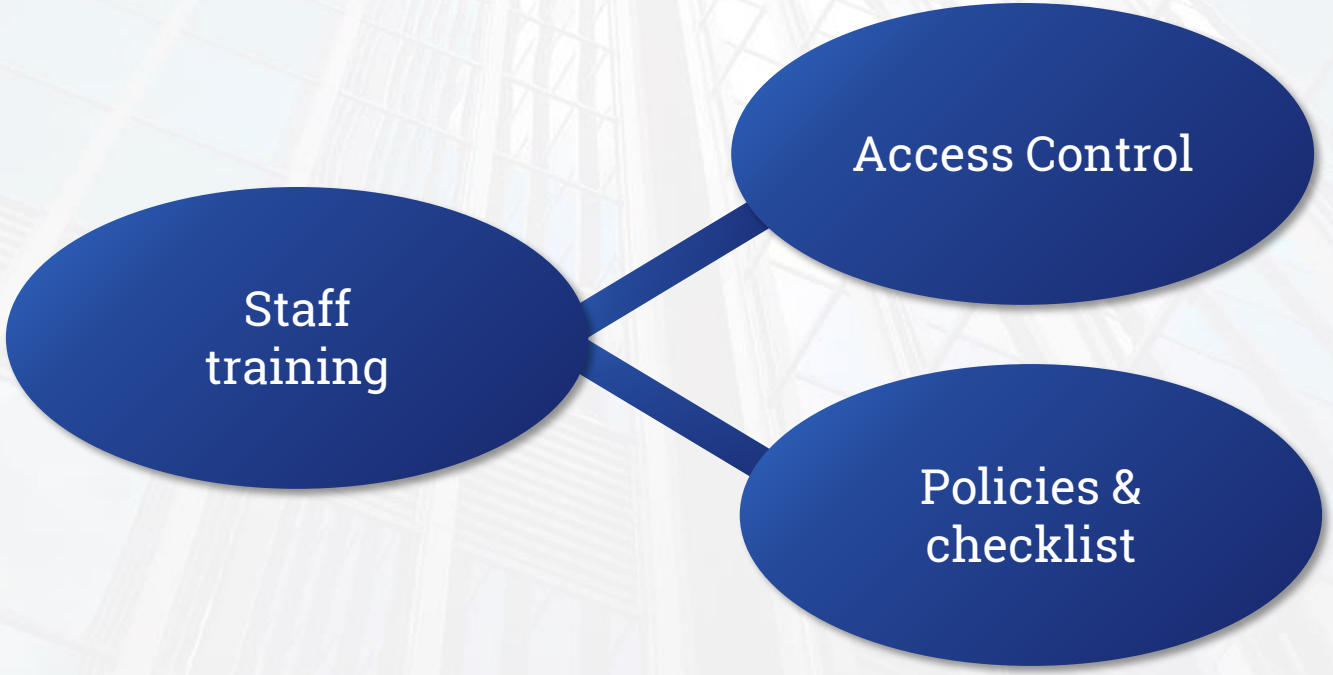
6 QUESTIONS TO ASK YOUR BROKER ABOUT CYBER INSURANCE

1. Is it an extension to an existing policy or a separate policy?
2. Are there any excesses and wait periods before your claim can start?
3. Do coverage and limits apply to both first and third parties? e.g. if you are a data controller and a third-party processor has a breach?
4. Does the policy cover
    - any attack which may be untargeted in deployment? e.g. WannaCry.
    - non-malicious actions taken by an employee? e.g. inadvertent execution of a file which causes damage.
    - against rogue employees?
    - social engineering as well as network attacks?
    - Terrorism and Cyber Warfare
5. Does the policy include for long term incidents ?
6. Does the Policy have post-breach support such as forensic, public relations firms and legal support?

SWCSC
SouthWest Cyber Security Cluster

PROTECT

Limit cyber incidents in your organisation



SWCSC
SouthWest Cyber Security Cluster

INTRODUCTION TO PROTECT

Protect focuses on reducing the risk of cyber incidents impacting on your business

- Logins and passwords
- Awareness training
- Policies & procedures
- Housekeeping
- Ways to use protective technology

SWCSC
SouthWest Cyber Security Cluster

KEY QUESTIONS:

- Who's got access to what information in my business?
- What's our training like?
- Do we have the right policies for protecting our data?
- Do I have a strong password?
- Who's got access to sensitive information in your business?
- Is the right data encrypted?

SWCSC
SouthWest Cyber Security Cluster

THE BASICS

Get into good habits – Update everything and everyone

Browsers

Mobile Phone Operating Systems

Email Software

Any Software

Website Software
(be careful if you have additional plug-ins, check with your developer)

Staff awareness & good practice training & monitoring

SWCSC
SouthWest Cyber Security Cluster

CONTROLLING ACCESS TO YOUR SYSTEMS

Access Control

A guide to access control methodology can be found here:

https://searchsecurity.techtarget.com/definition/access-control

Download new user checklist
Download leaver checklist

Download Access Permission Register

If you control access to your systems, you can minimise the risk of unauthorised access from staff and attacks. You can do this by...

- Limiting user file access based on the users role. Check when staff leave or change roles.
- Encrypting all devices that leave your premises (laptops etc)
- Enabling VPNs when working remotely
- Enabling Multi-Factor Authentication to Cloud Applications
- Splitting Networks for Internal/External Users

SWCSC
SouthWest Cyber Security Cluster

EMAIL SECURITY

The vast majority of cyber attacks will come via email as a Phishing attack

Have you implemented mail filtering software?

Are your emails encrypted?

Have you trained your staff on safe email use?

Remember to also secure your mobile and PC

Think about home PC security too

[Guide to email encryption]
[Guide to Email Filtering]
[Sophos phishing email training]

Reasons:

- Protect email content from prying eyes
- Reduce fake email from your domain
- Limit fraud

SWCSC
SouthWest Cyber Security Cluster

STAFF TRAINING ESSENTIALS

Human error accounts for 90% of cyber incidents

Staff awareness and training guides

https://www.itgovernance.co.uk/staff-awareness

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

Cybersafe offers a tailored training solution to your employees https://www.cybsafe.com

Free resource https://www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-overview?active-tab=description-tab

Make sure that ALL of your staff have a good level of cyber awareness

Keep training regularly

Test your IT plans with Simulated Exercises

SWCSC SouthWest Cyber Security Cluster

CHECKLISTS & POLICIES

Device Security Checklist

1. Are your Operating Systems and applications patched regularly?
2. Are you using a secure password and Multi Factor Authentication?
3. Have you got Anti-virus software & Encryption software in place?

Use of WiFi Policy on work computers

Ensure your policy includes:

- VPN use when outside of the premises
- Ways to limit file sharing
- Identification of legitimate wifi network
- If in doubt use your phones mobile data for connectivity
- Make sure you use a reputable VPN
  - https://www.ncsc.gov.uk/collection/small-business-guide/keeping-your-smartphones-and-tablets-safe

Privacy

Call the Information Commissioners SME Helpline for queries on the GDPR (the main privacy regulation) or the PECR (the marketing & comms privacy regulation) It's an excellent service

0303 123 1113
www.ico.org.uk

Laws like the GDPR are not about making life difficult, they are about protecting your company brand.
The greater your compliance the greater people can trust your business and the more data they'll share with you

Privacy is not about the law.
It's about your attitude and company culture towards the use of other people's assets - the data about them.

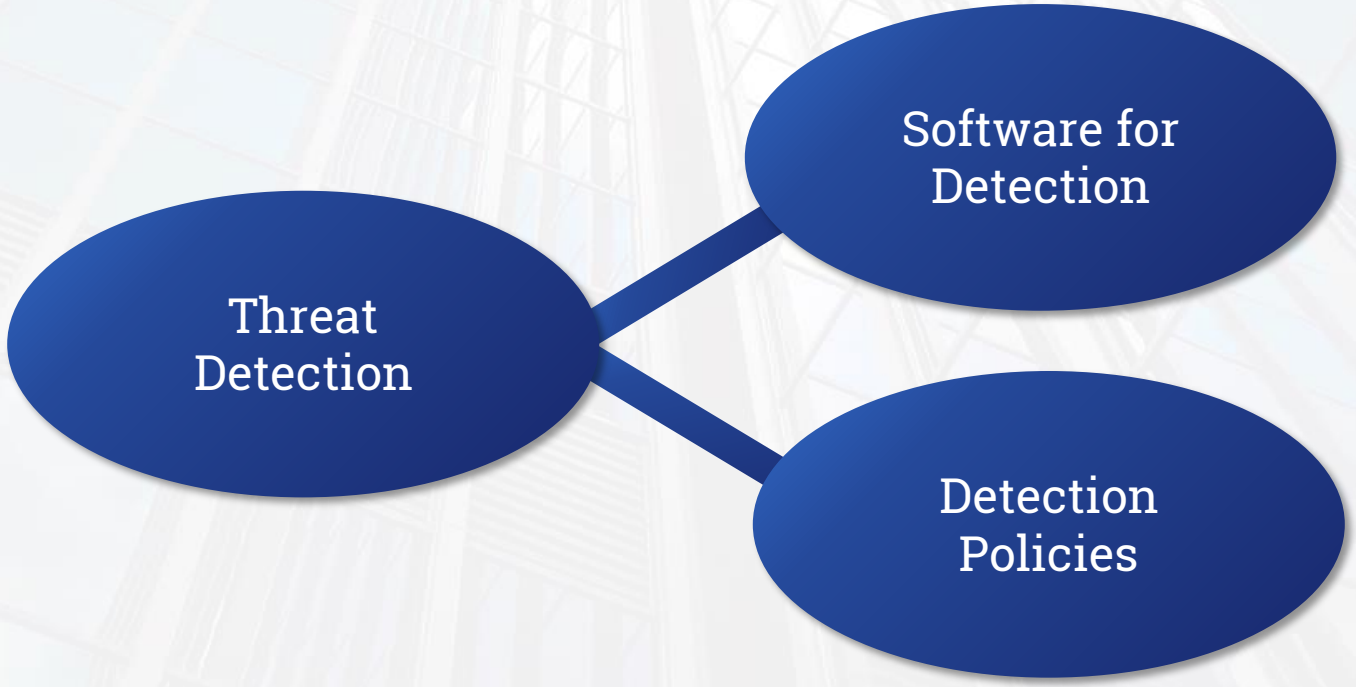
This document highlights principles and rights enshrined within the law. Understanding and seeking to comply with these objectives will put you on the correct path towards legal compliance.

Privacy Guidance - Basic 1st Steps

SWCSC
SouthWest Cyber Security Cluster

DETECT

Spot incidents early & identify mistakes in you organisation



SWCSC
SouthWest Cyber Security Cluster

INTRODUCTION TO DETECT

At the simplest level, it might be your staff realise that they've exposed sensitive personal data through an error, or it might be network snooping that lasts for many months.

- Anomalies & events
- Ongoing monitoring
- Detection processes

SWCSC
SouthWest Cyber Security Cluster

KEY QUESTIONS

- How do I spot a breach?
- Are we making mistakes and losing our data?
- Are there people already in our systems?
- What looks suspicious?

THREAT LANDSCAPE - WHAT ARE THE THREATS?

Threats are constantly changing, so review the threats frequently.

Review your Cyber Policies at least annually to check they match the evolving threats.

Keep up to date on threats with the NCSC: https://www.ncsc.gov.uk/report/weekly-threat-report-13th-december-2019

Top 5 threats to SMEs:

1. Phishing
2. Insecure passwords
3. Network vulnerabilities
4. Website vulnerabilities
5. Mobile malware

SWCSC SouthWest Cyber Security Cluster

THREAT DETECTION

How can I detect a data breach?

Do your research- find out the latest threats on a local and global scale to be aware of your most likely issues.

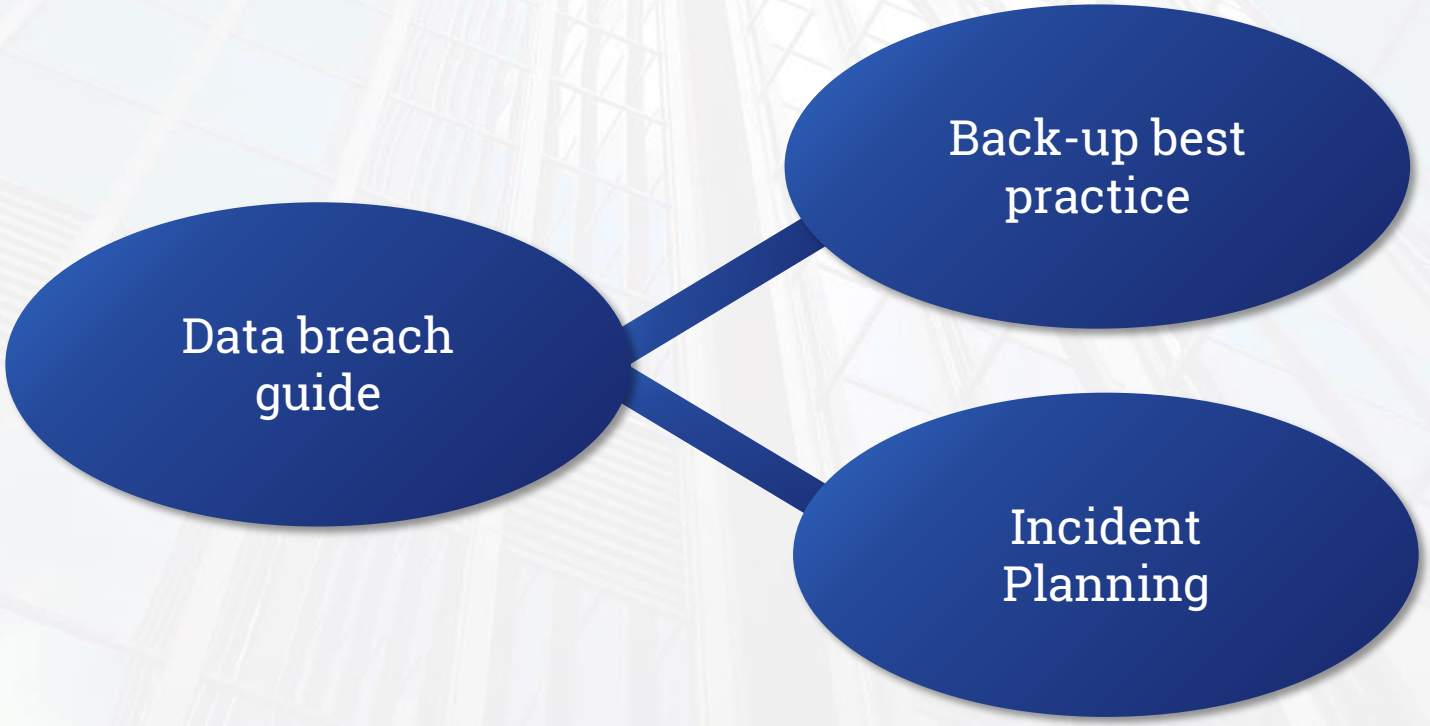
Monitor your organisation - ensure you have professional Anti-Virus software that will monitor your networks, logs and events from applications and security systems.

Possible warning signs

- **Slow systems** - might indicate malware or bulk uploading of files
- **Spam emails** - multiple spam emails might indicate a focused attack
- **Web statistics** - a sharp increase in web visitors might indicate a cyber threat
- **Other flash points**
  - Staff leaving
  - Unhappy staff or contractors

RESPOND

Minimising the impact by developing a response plan



SWCSC
SouthWest Cyber Security Cluster

INTRODUCTION TO RESPOND

Respond is about dealing with the incident(s)

- Response Planning;
- Communications;
- Analysis;
- Mitigation;
- Improvements.

KEY QUESTIONS

- What's gone wrong?
- What should we do when it goes wrong?
- Who do I inform?
- How do I respond with GDPR?
- What do I say to my staff and customers?

BACK UP BEST PRACTICE

Back up regularly - you never know, when your systems will be compromised!

Back ups help you to recover after

- cyber attacks, e.g. ransomware
- physical theft, stolen laptop
- lost hardware, lost laptop
- broken hardware

Core Back Up Policy

- How many days of data can you afford to lose - this is your maximum backup interval
- Consider weekly backup
- Test your restore procedure monthly
- Follow the 3-2-1 rule:
  - keep at least 3 copies
  - keep 2 copies on different media
  - keep 1 copy offsite and offline
- Understand the backup policy of your cloud services

SWCSC
SouthWest Cyber Security Cluster

5 QUESTIONS TO ASK YOURSELF OR YOUR SERVICE PROVIDER ABOUT BACK UPS

1. Which of your devices (e.g., your mobile) and cloud services are containing data/information that you cannot afford to lose?
2. Do you know, when a backup was not successful?
3. You long does a recovery take?
4. How much do you lose, if one individual backup is corrupt (cannot be restored)?
5. How reliable and accessible are your backup media?

SWCSC
SouthWest Cyber Security Cluster

INCIDENT TEMPLATES

Keep a register for incidents to help you track and check that the problems are fixed
Allocate a responsible owner
Review frequently to check you are resolving problems and making improvements

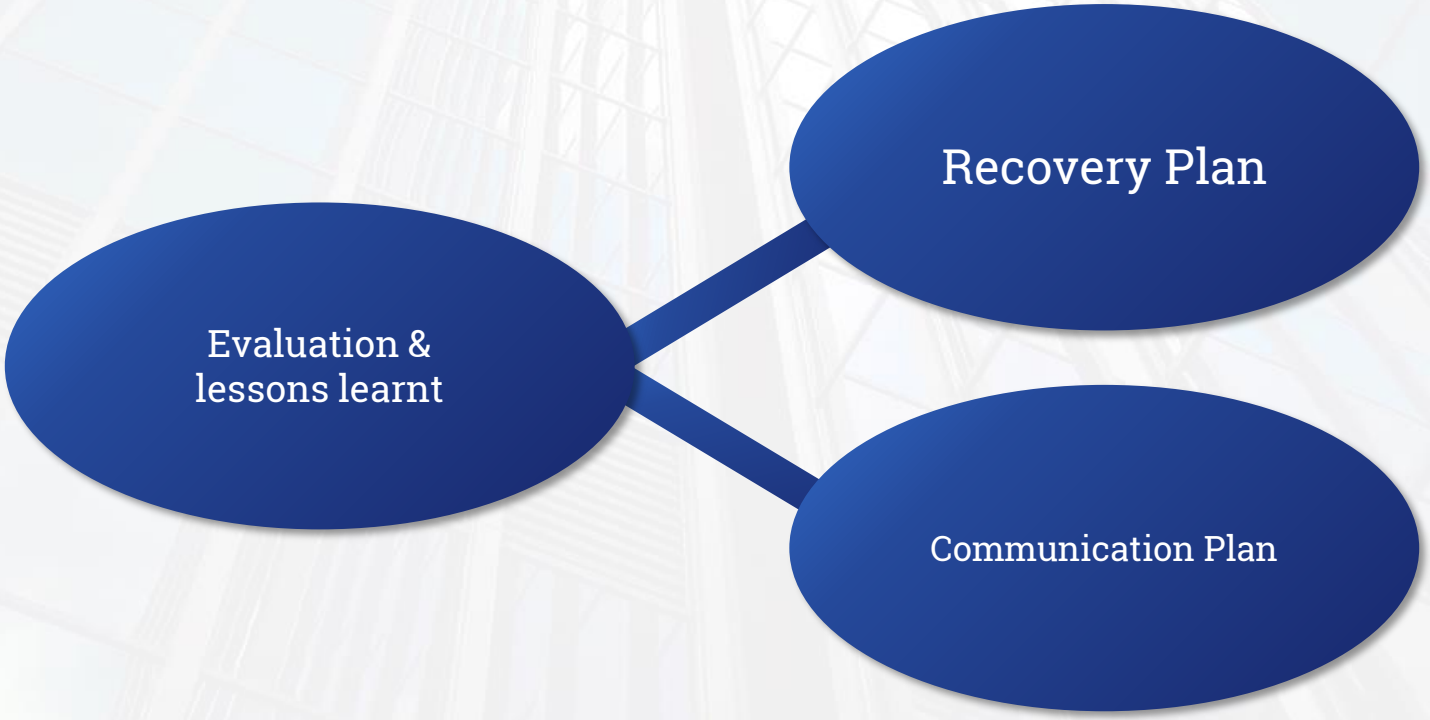
Incident Ref #	Date	Reported by	Affected System/Asset	Incident detail	Resolution	Residual Action

Download the Incident Template here

SWCSC
SouthWest Cyber Security Cluster

RECOVER

Getting the organisation back up and running



SWCSC
SouthWest Cyber Security Cluster

INTRODUCTION TO RECOVERY

Recovery is about getting your business back working and learning the lessons for the future

- Recovery planning;
- Improvements;
- Communication.

SWCSC
SouthWest Cyber Security Cluster

KEY QUESTIONS

- What did we learn from the incident?
- How can we do better next time?
- How do I regain confidence in the business?
- Have we tested our back up restore capability?

INTERNAL COMMUNICATIONS PLAN

Other's past experience demonstrates it's crucial to be open, honest and very timely

Develop & communicate positive messages on lessons learnt & improvements

Key questions:

Who do I need to tell?
How shall I report to my board?
How promptly can I tell them?

Visit this site for guidance on developing a comms plan

https://www.local.gov.uk/our-support/guidance-and-resources/comms-hub-communications-support/cyber-attack-crisis

SWCSC
SouthWest Cyber Security Cluster

RECOVERING FROM BACKUP

Having a Backup is one thing, but have you tested they work and that you can recover your data in a suitable time to suit your business requirements?

If recovering due to Malware have you got enough recovery points to select a date before the Malware?

(Please note that if you are trying to recover from a Malware attack then this can lay dormant on your systems for months/years so make sure you do not recover from an infected backup)

Remember that if you are recovering from a backup, it could be on different systems/hardware than you normally use so it is worth testing this.

Backups are sometimes your only Safety net, Make sure it works!

SMALL STEPS - BIG CHANGE

Small steps can lead to a big change

- build it up
- get people on board
- show some leadership
- share the good news
- track your progress & use it for evidence

Download the Toolkit Checklist here to help track progress!

SWCSC
SouthWest Cyber Security Cluster

WE WOULD REALLY VALUE YOUR FEEDBACK

To help us help you and other businesses, it's very important that we understand your views and experiences when using this toolkit.

Please take some time to tell us how you got on using it.

- Was it interesting, relevant and useful for you, if so in what ways?
- Was it difficult - too complicated, too technical?
- Is the toolkit missing something - if so please tell us what?
- Could the toolkit be better?
- Finally, have you had any cyber security related experiences, good or bad, that you would like to tell us about?

Tell us on-line at https://southwestcsc.org/contact/

SWCSC
SouthWest Cyber Security Cluster

ACKNOWLEDGEMENTS

This toolkit is based on the NIST 5 steps, for more information visit the NIST site https://www.nist.gov/cyberframework/online-learning/five-functions

With thanks to the South West Cyber Security Cluster Steering Group

Authors: Robin King, Bob Bunney, Roz Woodward, Geoff Revill, Kate Doodson, Darryn Knowles, Anthony Odhams, Durgan Cooper, Achim Brucker, Peter Jones

Version 2 - December 2019

Disclaimer: All information has been developed in good faith, the Cluster nor any members can be held responsible for any actions or incidents as a result of utilising the content or links on this toolkit. If any links are no longer valid or information incorrect, please email us info@southwestcsc.org.

Slideshow produced by MediaBadger

www.mediabadger.uk

SWCSC SouthWest Cyber Security Cluster

CONTRIBUTORS

BAR Associates

SECURIOUS

cosmic

Krowdthink

BLUELOOP

UNIVERSITY OF EXETER

SECUREARM CYBER SECURITY SERVICES

UNIVERSITY OF PLYMOUTH

SWCSC SouthWest Cyber Security Cluster