Business Resilience

Going beyond Cyber Essentials

Resilience through “people” controls

What are “people controls”

- Through advice, guidance, and certification, **Cyber Essentials** deals effectively with **technical controls**
  - “only” 80% of attacks thwarted (pretty good start!)

- “User Controls”
  - SME needs to know what their people should do
  - then train them to do the right thing!
  - policy needs to include responsibility for digital behaviour
- “Management Controls”
  - instilling the culture and proving the mechanism to enable people to do the right thing

Which people? And what can they do?

- User controls apply to ALL employees and contractors
  - have to know (training) what to do and be tested accordingly

- Management controls could apply to
  - IT managers
  - HR
  - Finance
  - Departments
  - Senior Management

IT people (**in-house** or **from IT provider**) are great at setting up and general maintenance

- may not be good at “soft skills”

HR? (linking contracts, policies, responsibilities – including with IT providers)

- may lack IT skills

Finance? (provide a budget for cyber security, separate from IT provider fees)

- Understand IT, good example for others, role in training?

Managers (control user behaviour through policy and liaison with IT regarding technical controls)

- Need to work with all of the above…

People controls are essential to identify “who is responsible!”

Two “disaster”/lack of resilience scenarios:

Scenario 1: System no longer works!

Scenario 2: Data is lost/stolen!

Scenario 1: System not working

- Could easily be an IT cock up
  - Hardware failure?
  - Software failure?
  - **Resilience…** in each case should be backup

- Could be Internet or Electricity Provider failure?
  - Backup supplier (e.g. 5G)
  - Backup battery or generator…
  - **Resilience?** IT or management/finance not providing funding

- Management Responsibilty… no trading; lose business

Scenario 2: Data Lost/Stolen

COULD be an IT failure, or IT provider failure…

- More likely, a failure of
  - understanding with IT manager/provider
  - HR (lack of systems, user training)
  - finance (no budget for training/systems)
  - management (system/training ineffective, limits user behaviour)
- All the above carry **Senior Management responsibility!**
  - Same consequences regarding no trading…
  - **ALSO** must by law report breach to ICO
    - **ICO** will investigate who is to blame…
    - if responsibility can't be determined… system failure!
    - insurance companies may not pay out for "negligence"…

Scenario 2: IT Providers set things up/configure (but can't control users!)

Organisations that embrace Cyber Essentials properly (i.e. with management oversight) need to help out (share responsibility):

- **Devices/software**. Make sure:
  - employees/contractors don't have software on their devices that is not needed for the business
  - all software is updated within 14-days of a new version becoming available
  - auto-updates system is working…

- **Firewalls.** Make sure:
  - someone knows how to change the admin password
  - Management policy for approving opening/closing ports (some software needs to have a port open to work). An issue of RISK!

- **Anti-malware software**
  - needs to be active (and up to date!)

IT Providers & Business “users”?

(can’t control everything…)

- Organisations that do Cyber Essentials properly (i.e. **with management oversight**)
  - find that several people need to be involved in answering the questions
  - gets them thinking about “people controls”

- If they use an external IT provider (or MSP), must involve an outsider
- If they use an IT manager AND an MSP, both, plus management need to be involved

Controlling IT, & Controlling Users is NOT an IT provider responsibility

- **Employees are People…**
  - most are long-term computer users
  - don't like being told about IT matters
  - may think they know it all?
  - need dialogue
  - otherwise could become "sneaky" (not following policy)
  - known as "**shadow IT**")

Behaviour Control "Carrot & Stick"

- Regular education/training/testing including reminders about passwords, updates, phishing
  - something in the employment contract
  - USE Information Security policy

- **Listen to people** when they talk about software they used at college/in their last job etc.

(could be beneficial – if so, maybe everyone in the business could benefit, let them explain)

IT Providers Responsibilities...
v
Company Responsibilities...

- **Service provider:**
  - does IT supply/set up/config
  - MAY offer cyber advice or (if CE savvy) management of controls

- Need a **contract**
- Need a **list of tasks** for each
- **Probably need legal advice!**

- **ICO makes it clear that loss of data is a company responsibility**

IT Provider or MSP?

- The terms overlap
- MSPs tend to be larger, offer more services
  - may include Cyber Security advice, and taking SMEs through Cyber Essentials
- IT Providers small, even sole traders
  - tend not to be cyber security specialists

- This matters: new CSR Bill applies to 50+ employee organisations only, policed by a new regulator…

Possible Agreement between MSP/IT Provider and SME

- MSP agrees to provide, maintain equipment and software, and to attend and fix within an agreed time
- SME agrees to manage staff training as appropriate to ensure that MSP equipment and software are used correctly
- SME agrees to maintain a Cyber Security policy covering all aspects of use of IT facilities provided by the MSP
- SME agrees to seek advice from MSP on matters relating to Cyber Security policy and to to achieving and renewing Cyber Essentials

Who looks after your organization's Cyber Security?

- IT Providers/MSPs are everywhere
  - provide a vital, excellent, and patient service to make SMEs function digitally
- Cyber Security Experts aren't commonplace
  - why assume your IT Provider also does Cyber?
  - an MSP is more likely to have the skillset…
  - ask: do they have Cyber Essentials?
- If there's a gap in the contract…
  - find a way to fill it!