RICHARD HENSON, DIGITAL DEVON

Making SMEs more Cyber Resilient

rēgola

A Devon NCSC Certification Body

We've signed the Cyber Resilience Pledge

New UK Legislation (Cyber Security and Resilience Bill)



Work began in 2024. Expected to become an Act of Parliament later this year...

https://bills.parliament.uk/bills/4035

What does this mean for SMEs?

Cyber Security & Resilience Bill

Why more legislation?

- too many businesses offline, too much of the time! 43% had been hacked in 2025
  - https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
- affecting GDP and prosperity of the nation!

Can do better!

- Internet-based digital supply chains for over 20 years
- plenty of good advice available
  - too much is ignored
  - few signs that SMEs are doing the right things to protect themselves

Legislation seems the only way...

Cyber Security & Resilience Bill

How to protect Digital Business!

- improve awareness and encourage certification
- strengthen supply chains (no more “weakest link” businesses)
- regulate MSPs (Managed Providers/IT Providers)
- encourage SME senior management to **take responsibility** regarding IT failures and Data Breaches

Where to start? 1. Responsibility

- Confusion about IT infrastructure responsibility and Cyber Security Responsibility
  - businesses handle personal data
  - responsibility under UK GDPR, 2021

- Pay MSP for a service?
  - BUT unrealistic for MSPs to take responsibility… therefore boards must!

Where to start: 2. Awareness

- Digital data is potential money, to hackers
  - hackers now have AI tools making them even more dangerous
- On-line business systems an easy target
  - especially businesses that partner bigger businesses
- SMEs need to defend those systems and provide evidence that they do!

Where to start: 3. Validate Systems

- Validation implies external approval
- Easiest way: get certified (c.f. CORGI gas installer)

- Equivalent for SME Cyber Security is Cyber Essentials (CE)
  - 2025 survey showed that only 12% knew enough about this standard

- Only a first step towards Cyber Resilience…
  - only validated with external testing (CE+)

Last 20 years: “hands off” approach… Why regulation NOW?

- More UK companies are being attacked than ever!
  - supply chains more at risk than ever
  - existing strategies not sufficient
    - https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
- Once attacked, companies can take a long time to recover
  - If too long, they’ll go out of business…
- Two pronged approach needed
  - Stage 1: defend systems well
  - Stage 2: prepare for a breach, and prepare to bounce back afterwards!
- A resilient system can be attacked… and can recover quickly

The SME “problem”?

- Since the 1980s, businesses encouraged to be free thinking and independent: “red tape” perceived as holding them back…
  - “light touch” works in some areas, where there is good understanding of long understood principles
  - unfortunately, IT and Cyber Security are still quite new
    - good “misunderstanding” ☹
    - people need to use & share **trusted sources**

The “Resilience Framework” (NCSC)

- New standards do need to be accepted & regulated…
  - 1965: Seat belts fitted to cars, for safety. Many didn’t wear them
  - 1984: Seat belt law… well enforced. Everybody wore them!
- Cyber Security as the new “safety”?
  - Cyber Essentials started in 2014…
  - Resilience Law, 2026 or 2027
  - Cyber Resilience by 2029 looks optimistic…
  - **Urgency** needed!!!

“Defend Together!”

BUT…

- **Every user** presents a potential risk…
  - hacker guesses password (too short? Not MFA?)
  - computer they are using not properly configured (out of the box?)
  - firewall to/from the Internet not properly configured (as above?)
  - updates off, or not updating

- **Larger companies** use IT staff to look after “Technical Controls”
  - make sure these are working (best if externally tested e.g. Cyber Essentials (CE), CE+, ISO)
- **Smaller companies** may rely on an “IT guy” (NOT a cyber expert)
  - no guarantee of cyber security
  - may be unaware of CE. But should have CE+ (?)

How to Defend your systems…

“process-based”

Everyone’s Responsibility!

Computers, and their software, have excellent technical controls

Companies need to make full use of the technology in their systems

- operating systems
- firewalls
- antivirus
- access control

All need maintaining and updating! Not just an IT problem… involves everybody

- get certified for the combined effort!

“Everybody’s Responsibility?”

BUT…

- **Most SMEs (especially smaller ones) STILL see cyber security as an IT problem**
- **Small/medium** will have an IT specialist (e.g. IT manager)
  - IT manager looks after cyber (?)
- **Microbusinesses** often rely on an external “IT guy” (NOT a cyber expert)
  - buy in the service
  - no guarantee of cyber security
  - may be unaware of CE. But should have CE+ (?)

What is this "Cyber Essentials"?

A technical security standard, developed by GCHQ in 2014

Why don't SMEs all know about it?

- Other standards were already available (e.g. ISO27001)
  - expensive
  - not designed for, or suitable for, SMEs
    - distrustful of standards
    - only followed them if had to
    - many didn't engage

So… what is Cyber Essentials?

- An inexpensive “UK only” solution originally developed by GCHQ
  - focus on five technical controls
  - testing based on a series of questions
  - **80% effective** for SMEs who get certified
- Cyber Advisor
  - explains the questions and relates them to the SME
- Cyber Essentials Assessment
  - tests five technical controls
  - awards certificate (in most cases…)
  - unlocks insurance cover
- Retested 12 months later. Questions tweaked each year.



Where do I go to get Cyber Essentials?

- IASME control Cyber Essentials assessment and certification on behalf of NCSC
- http://iasme.co.uk/cyber-essentials
- Two routes available…
  - allocation via payment and allocation to the IASME “pool”
  - allocation by direct contact with a Certification Body (CB)
    - CB list available at: https://iasme.co.uk/network-directory
    - CBs that are also Assured Service Providers provide a free 30 mins consultation with an NCSC-endorsed Cyber Advisor.
- You answer questions on a “portal”, get it signed off by **senior management**, and an assessor marks your work. You get 48 hours for “corrections”.

What about the other 20%?

- Not everything can be under technical control!
- Input/output often has to be via **human**!
  - controlled through policy, contract, and training
- People make mistakes
- People can go “rogue”
- People can be deceived (or “socially engineered”)
- **Conclusion:** no system can be 100% secure

If CE doesn't cover the "people" part, what use is it?

Technical security should be the easy bit. But, after 12 years, only 3% of SMEs have Cyber Essentials certification...

No standard can control people effectively!

- **organisations,** through their policies, are about controlling people!

BUT... Cyber Essentials asks 85 questions: forces the organisation to at least **think** about the people issues