

October is International Cyber Awareness Month

- Cyber Awareness is the first step
- It is necessary for an organisation to realise the importance of **Defending Their Systems** to meet approved standards
- Regola are offering Cyber Essentials at 15% discount
- Orders by midnight on 31st October





A Cost-Effective Path towards Cyber Resilience?



Regola Digital Consulting

An NCSC Certification Body

We've signed the Cyber Resilience Pledge



Business Resilience... and Cyber Resilience

Much interest in tools to make the business more efficient and responsive to change (survive/flourish in a competitive environment)

All businesses now digital so they should also be well-defended and responsive to digital threats (**bounce back after an attack!**)

New UK Legislation (Cyber Security and Resilience Bill)

Expected to become an Act of Parliament later this year...

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

Focus on:

- protecting supply chains (no more “weakest link” businesses)
- MSPs (Managed Service Providers/IT Providers)

Current confusion about **IT infrastructure responsibility** and...

Cyber Security Responsibility

unrealistic for MSPs to take responsibility... therefore boards must!

Cyber Essentials and Cyber Resilience

- **Cyber Essentials**

- 5 technical “controls”, using existing technology
<https://www.ncsc.gov.uk/cyberessentials/overview>
- 80% effective! (people - other 20%)
- £25000 insurance cover
- Delivered through Certification Bodies

- **Cyber Resilience**

includes Cyber Essentials (or equiv.); goes several steps further

- User controls
- Management controls
- Third Parties (especially supply chain partners)
- Acceptance of Cyber Security as the responsibility of Senior Management

Cyber Security
is “process-
based”:

Everyone’s
Responsibility!

Focus set by
Management

**Cyber Security is system, made up of
processes**

NOT a product

- Everyone needs to;
 - understand their role
 - get regular reminders and training on changes
- Individual items of system checked regularly
 - Cyber Security Budget for people, and policy, not just hardware/software
- Whole system checked? (once a year?)

IT Provider Responsibilities

...

and Company Responsibilities

IT Providers set things up (but can't control everything!)

Organisation needs to check (e.g.)...

- **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
 - company maintains responsibility for 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!)

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)

Importance of Partnership!

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...

Who is
Responsible if

- data is lost/
stolen!
- system
doesn't work?

- Answer... **Senior Management**
 - COULD BE “IT failure”
 - More likely, a failure of
 - understanding with IT provider
 - HR (systems, user training)
 - finance (budget)
 - management (system setup, user behaviour)
 - Must report breach to ICO
 - **they** will investigate who is to blame...
 - Insurance companies may not pay out for “negligence”...

Resilience Solution (UK wide?)

- **Sort out technical controls**
- **Sort out users, and management of business continuity procedures**
- **Sign the “pledge”**
<https://www.gov.uk/government/publications/cyber-resilience-pledge>
- **Management takes responsibility where IT Provider falls short (identified via contract!)**
- **Weed out “weak link” supply chain partners** <https://iasme.co.uk/cyber-essentials/ncsc-certificate-search/>
- **THEN...**
 - **hackers will have a difficult time!!!**

How long until we are “resilient”?

- **Much to be done:**
 - MSPs (IT Providers) work constructively with SMEs...
 - Objective: Cyber Essentials across Supply Chains (no weakest link!)
 - Companies with Cyber Essentials work towards Cyber Resilience **compliance**
 - Objective: SMT accept responsibility for Cyber Security (**and breaches**)
- **Like all IT regulations, The Cyber Security and Resilience Act will have two years to bed in...**
- Enforcement from late 2028...

Will a Resilience Framework be enough?

- New standards do need to be regulated...
 - 1965: Seat belts fitted to cars, for safety. Many didn't wear them
 - 1984: Seat belt law... everybody wore them!
- Cyber Essentials started in 2014...
 - Is cyber security the new “safety”?
 - Will a 2026 law be enforced?
 - Cyber Resilience by 2029 looks optimistic...



Thank You.

Questions?

**An NCSC Certification Body
And Assured Service Provider**

hello@regola.co.uk

Website: <https://regola.co.uk>

We've signed the Cyber Resilience Pledge

15% discount on Cyber Essentials this month