**Cyber Awareness, Security, and Resilience**

Version 1.0

**Contents**

[**1.** **Cyber Awareness** 3](#_Toc76567550)

[**2.** **What is the Internet of Things (IoT)?** 3](#_Toc76567551)

[**3.** **What is Cyber Security?** 4](#_Toc76567552)

[**4.** **What is Cyber Resilience?** 5](#_Toc76567553)

[**5.** **Steps to Cyber Resilience** 5](#_Toc76567554)

[**6.** **Factors Affecting Cyber Resilience** 5](#_Toc76567555)

# **Cyber Awareness**

Educating your staff by making them aware of the cyber risks they face, embedding basic controls, upskilling as necessary, and creating a supportive culture backed by robust policies and procedures, will improve your security.

Cyber awareness means that staff:

* **Know** what type of risks they face.
* **Understand** what is necessary to mitigate them.
* **Act** when necessary to report or reduce risk.

System users form the best defence from cyber-attack. Conversely, users are also one of the highest risks to your network due to human error, fraudulent communications such as email, and failure to protect access credentials such as passwords. Severe security and data breaches are most likely to be caused by the human factor.

# **What is the Internet of Things (IoT)?**

The Internet of Things is a term used to describe the ever-increasing number of devices which connect to the internet.

Our lives in the physical world are merging with the lives we lead online, through online shopping, gaming, work, and study. This means that smart phones, heating controls, and even toys if they connect to an app, will form part of the Internet of Things (IoT).

As devices become more affordable and more efficient, their use grows exponentially. As connectivity becomes more embedded into our everyday lives, ‘smart’ devices are making it easier to connect to the internet, wherever we are. Predictions on the number of connected devices estimate that they will exceed 50 billion by 2024.

In order to secure devices, settings must have complete, up-to-date inventories of their hardware and software. It is impossible to assess the risk if there is no asset management.

# **What is Cyber Security?**

Cyber security is the protection of devices, systems, and networks by implementing measures focused on preventing theft, damage, information disclosure, or corruption.

Cyber security centres on keeping unauthorised persons out. Security can involve one layer or many layers. A ‘layered’ approach is more secure, but nothing is 100% effective.

Implementing Cyber Essentials basic controls will prevent the majority of unsophisticated attacks, but prevention is never guaranteed.

Cyber security measures alone are not enough to protect and prepare settings from the escalating number and severity of attacks.

|  |  |
| --- | --- |
| Example Threat | Example Security Methods |
| Unauthorised access | Unique usernames and passwords / encryption / software keys / Policy |
| Theft | Site security barriers / locks / secure storage / CCTV |
| Data corruption | Anti-virus / malware protection / firewalls |
| Data disclosure | Identity verification / role specific access / digital signatures |

Cyber security forms *part* of cyber resilience.

|  |  |  |
| --- | --- | --- |
| **Data Security** | **Cyber Security** | **Cyber Resilience** |
| Data Security is the protection of data from accidental or deliberate unauthorised change, destruction, or disclosure.  Data security can cover hardcopies, such as files in filing cabinets, and disclosure of information through images and unique identifiers, such as your IP address.  Data security also covers secure data transmissions. | Cyber Security is the protection of computers, electronic communications, systems, networks, and the data those devices and systems contain.  Cyber security aims to ensure information integrity, accuracy, and confidentiality is maintained and systems are always available. | Cyber Resilience is the protection of data and systems to ensure reliable, consistent, and secure access to systems and data.  Resilience also encompasses the need for organisations to:   * risk assess systems * mitigate potential risks * respond to incidents * recover from attack or disaster promptly   The aim is to preserve **data and system** integrity and the confidentiality of **personal and organisational** data. |
| **Data security forms part of data protection.** | **Cyber security supports data security and forms part of cyber resilience.** | **Cyber resilience includes data protection, data security, and cyber security.** |

# **What is Cyber Resilience?**

Cyber resilience enables your setting to continuously deliver education and to carry out school business effectively, securely, and with prompt recovery in the event of an incident.

Cyber resilience involves preparing and responding promptly and effectively when incidents occur and adapting to ensure business continuity and enable recovery.

Cyber Essentials can help you reduce the likelihood of cyber-attacks and provide free cyber liability insurance. Cyber security is an integral part of cyber resilience, but resilience is an ongoing journey.

# **Steps to Cyber Resilience**

* Processes and procedures
* Security and protection
* Preparation and planning
* Monitoring and detection
* Incident response and recovery

All of these should be underpinned by whole site awareness and appropriate, role specific training.

# **Factors Affecting Cyber Resilience**

* **Culture:** The belief that cyber security is an IT issue, not relevant to educational settings, and a sense that cyber incidents are unlikely can lead to poor cyber hygiene.
* **Compliance:** Failure to use adequate technical and organisational controls to protect sensitive data can lead to breaches of the data protection act 2018 and UK GDPR.
* **Cost:** A lack of investment in data security can lead to escalating recovery costs, reputational damage, and fines relating to breaches.
* **Change:** Failure to plan appropriately and assess new systems prior to implementation increases the risk of vulnerabilities and breaches.
* **Continuity:** Failure to plan for an incident and test the plan leads to difficulties in recovery and extended recovery timescales.
* **Cover:** Settings without insurance cover could be left without financial support to respond and recover from incidents.