LUCIDICA

HELPING A UK-BASED NON-PROFIT ORGANISATION BECOME CYBER ESSENTIALS CERTIFIED

CASE STUDY

OVERVIEW

A UK-based non-profit organisation in the education and human rights sector supports academic people who are facing danger, persecution, discrimination, or violence in their home countries.

Because of the sensitive nature of its work, the organisation needed to ensure its IT environment had strong baseline security controls in place. Cyber Essentials readiness became a priority to help demonstrate that the organisation was managing key cyber risks appropriately. The organisation had 25 users and devices.

CHALLENGE

The main challenge was helping the charity become Cyber Essentials ready in a practical and cost-effective way.

Before the work began, several security gaps needed to be addressed. Standard users had local administrator access, which increased the risk of accidental changes, unauthorised software installation, and potential malware exposure. Some operating systems also required updates, and there was a need to improve how devices, applications, user permissions, and security policies were managed.

The organisation also needed its wider IT security controls reviewed, including Microsoft 365 access, MFA, password policies, backups, domain security, endpoint protection, and user awareness.

For a small non-profit, the solution needed to be proportionate, manageable, and aligned with Cyber Essentials requirements without adding unnecessary complexity.

SOLUTION

Lucidica supported the organisation through Cyber Essentials readiness work using its Security Ultimate package. This was the most suitable option because the client wanted to improve overall IT security compliance while also working towards Cyber Essentials.

The work focused on identifying missing controls, improving existing protections, and adding tools where required.

Key actions included:

Access control and user permissions

Standard users had local administrator access, which created unnecessary risk around software installation, system changes, and malware exposure. Admin rights were removed from day-to-day user accounts to reduce the risk of unauthorised or accidental changes.

Operating system and application updates

Operating systems were brought under closer monitoring through a centralised RMM platform to reduce exposure to known vulnerabilities. Unused applications were also removed, as outdated software can create avoidable security gaps.

Microsoft 365 and account security

Password policies, user accounts, Microsoft 365 access settings, and MFA were reviewed and strengthened. Since Microsoft 365 is central to daily operations, tightening these controls helped reduce the risk of unauthorised access and supported Cyber Essentials requirements around secure authentication.

Domain and email security

Lucidica configured DMARC protection to prevent the organisation's domain from being used in spoofing or impersonation attempts. For a charity working with sensitive communities and external partners, this was a particularly important layer of protection.

Backup and data protection

Email and SharePoint backup protection were implemented using a dedicated cloud backup solution. This ensured the organisation could recover data if emails or files were accidentally deleted, compromised, or affected by a security incident.

Endpoint protection

Endpoint protection controls were reviewed and improved across the organisation's managed devices to strengthen protection against malware, ransomware, and other device-level threats. This was a key part of building a Cyber Essentials-ready environment.

Security policies

Lucidica reviewed and implemented the required security policies and helped ensure they were communicated internally. Formalising these policies made security expectations consistent across the team, covering device use, accounts, passwords, and applications.

User awareness and phishing visibility

Lucidica provided reporting on user security activity, including whether staff interacted with phishing simulations or clicked on phishing links. This gave the organisation visibility of where extra guidance was needed, without adding heavy processes.

Ongoing monitoring and support

Ongoing monitoring was set up through the same centralised RMM platform, covering areas such as devices being offline, full disks, and serious vulnerabilities. This meant potential issues could be identified and addressed early, rather than discovered after they caused disruption.

Cyber Essentials Assessment and Certification

Once the required security measures were in place, a Cyber Essentials assessment was completed by Lucidica's in-house assessor. The organisation achieved Cyber Essentials certification successfully and without issue.

OUTCOME

The organisation achieved Cyber Essentials certification successfully and without issue, following the readiness work and assessment completed by Lucidica's in-house assessor.

As a result, their overall cyber risk was significantly reduced across several areas:

- **Access control risk** was reduced by limiting unnecessary user privileges.
- **Phishing risk** was reduced through better visibility of user behaviour and risky interactions.
- **Email account risk** was reduced through stronger account security controls.
- **Email spoofing risk** was reduced, helping protect the organisation's reputation and communications.
- **Cloud data risk** was reduced, giving the charity better resilience against accidental loss, compromise, or disruption.
- **Employee behaviour risk** was reduced through clearer awareness of how staff respond to security threats.

CONCLUSION

Overall, the organisation moved from a higher-risk environment to a more secure, compliant, and manageable IT setup suitable for a 25-user non-profit.

For more information about Lucidica IT Support's services and how we can assist your business, please visit Lucidica website. Our portfolio of solutions extends beyond the restaurant industry, as we aim to empower businesses with reliable technology foundations.