BACKGROUND

Founded in 1950 by Sir John Wilson, Sightsavers is an international development charity that works to prevent sight loss and fight for disability rights in some of the poorest parts of the world. One of its outstanding achievements is to have been involved in delivering a billion eye treatments to tackle neglected tropical diseases. Outside of the staff employed in its head office in Haywards Health, Sightsavers has over 350 staff working in 30 countries, predominantly in sub-Saharan Africa, as well as Asia. One of Sightsavers' principal donors is the UK Foreign, Commonwealth and Development Office (FCDO) and it was a requirement set by the Office in 2017 that prompted Sightsavers to seek Cyber Essentials (CE) certification.

Developed as a part of the UK government's National Cyber Security Strategy, CE is a simple yet effective, government-backed framework designed to protect organisations from a range of the most common Internet-based cyber-attacks.

In order to achieve certification, organisations are required to address five basic control areas (access control, secure configuration, software updates, malware protection and firewalls and routers).

This case study highlights the challenges Sightsavers faced in achieving CE certification, how it overcame them, the benefits this had and some of the key lessons for other charities.

CHALLENGES

The first step for Sightsavers on its journey was to understand what was involved in achieving certification to CE. In order to address this, it approached URM Consulting (URM), a CE certification body and information security specialist, to conduct a CE readiness assessment. The readiness assessment focused on Sightsavers' level of compliance with the five main control areas.

One of the five control areas that CE requires organisations to address is 'software updates', which involves ensuring software and operating systems are regularly checked and updated with the latest patches to protect against vulnerabilities. In single site organisations, this can be a relatively straightforward task, but for a complex distributed environment it can represent a far greater challenge. For Sightsavers, at the start of 2017, with 30 offices spread across Africa and Asia (and staff working in the field using different technologies and different versions of software on different devices), this presented an even greater challenge. Software patches at that time were being installed by memory stick by the users themselves, relying on their goodwill and memories to apply them. Hardware installations were also being carried out by engineers flying to and from the UK.

Following URM's CE certification readiness assessment, it was clear to both parties that meeting the requirements of the 'software updates' control in particular was not going to be a quick and easy fix.

SOLUTION

A strategy was formulated where Sightsavers set short term goals to achieve CE certification with a limited geographic scope and then to expand to a global scope once the appropriate infrastructure had been implemented. Central to this strategy was the conscious and commendable decision of Sightsavers' Board not to treat CE just as a box-ticking exercise. The Board fully embraced the scheme and used it as an opportunity to transform the cyber security practices and to develop a more resilient IT infrastructure that would improve efficiencies and free up users from any IT admin tasks. As a result, Sightsavers has made a significant investment in time, money and effort to improve the usability of systems and endpoint security, including the following technical elements:

- Rolling out standardised laptops, all of which have been installed with Windows 10, BitLocker encryption, and anti-virus and firewall software. Sightsavers was also careful to avoid any bloatware scenarios by ensuring that the minimum necessary business software was installed on all laptops and any unnecessary software was uninstalled
- Implementing a centralised endpoint configuration management system in order to automate the patching process and provide monitoring and management of every endpoint
- Installing servers in 26 remote offices each with three virtual machines (domain controller, file server and distribution points for the configuration management system) in order to facilitate the downloading of patches
- Implementing a centrally managed and Cloud-based anti-virus solution

As Andrew Blackburn, Information Security Manager at Sightsavers, points out, the CE-inspired infrastructure investment was not just about technology solutions: "We recognised the importance of establishing policies and processes and raising awareness of security threats with all our remote users, who may be working from a regional office or from home." This foresight served Sightsavers extremely well during the current COVID climate, enabling any user to work from home productively and securely. Some of the key non-technical initiatives and enhancements

- Establishing a dedicated Information Security Team in 2018 headed by Andrew Blackburn, an experienced CISSP qualified Information Security Manager
- Developing and improving key operational and security processes, for example, a Joiners, Leavers and Movers Process, which led to improved access control and IT asset management
- Developing and delivering cyber security awareness exercises, for example, phishing exercises, which not only raised awareness of this particular threat, but have led to many users proactively contacting HQ with reports of phishing attacks; or as Andrew puts it, "Acting as our eyes and ears."
- Planning cyber and information security themed training events to raise awareness of common threats and promote the need for continued vigilance.

BENEFITS

> *Cyber Essentials has provided a very good base level for our cyber security and has had wide-ranging impact across systems and environments.*

Andrew Blackburn
Information Security Manager at
Sightsavers

Andrew Blackburn believes that "CE has provided a very good base level for our cyber security and has had a wide ranging impact across systems and environments."

The URM-supported decision to start with a smaller scope and expand served Sightsavers well by starting the journey with a tangible, achievable reward – CE certification. Andrew believes some of the more significant benefits associated with certifying to CE are:

- Major improvements to endpoint security, with all remote staff now using standard laptops and operating system software and with all machines having BitLocker encryption. All laptops have also been installed with AV and firewall protection. Also, by removing bloatware, Sightsavers has reduced the risk of breaching copyright and software licence agreements and improved laptop performance
- Vastly improved centralised management and monitoring of every endpoint, ensuring that all critical patches are installed in a timely fashion
- Greater efficiencies and cost saving, negating, for example, the need for staff to travel to Africa and Asia to install hardware
- Greater organisational resilience, as demonstrated by dealing with COVID-19. Sightsavers' investment has enabled every user to work productively and securely (every machine has always-on VPN connectivity) from home, even where there are connectivity capacity limitations
- Full engagement and commitment from the Board in cyber security, with an appreciation of the benefits to be derived
- Assisted in the compliance with other regimes such as PCI DSS and the GDPR, e.g. securing personal data at rest through encryption
- Providing reassurance to donors and partners on the protection of their personal data through Sightsavers' endpoint security controls and its policy of only keeping the absolute minimum amount of personally identifiable information. While CE is a UK-centric scheme (it has lower awareness in other parts of the world), Andrew Blackburn believes that regulations like the GDPR have greatly raised individuals' interest and concern in what organisations are doing with their data.

THE FUTURE

According to Andrew Blackburn “Cyber security is a never-ending journey with constantly evolving threats where organisations can never afford to rest on their laurels. However, CE has provided the ideal base level on which we can build and enhance our security stance.”

One example of this enhanced security is that Sightsavers is currently trialling a product that will enable users to pull down the latest patches from vendors wherever they are in the world.

LESSONS LEARNED

When asked whether he would recommend CE to other charities, the answer from Andrew was:

“Yes, absolutely. It is something that can be achieved by any organisation. The amount of effort will naturally depend on the existing infrastructure and size of organisation. At Sightsavers, with such a complex and distributed environment the investment has been significant, but so have the benefits. One of the great things about CE is that it is a targetable standard, so you always know exactly where you are. And even if it takes you a while to certify, you can quickly pick off some low-hanging fruit (like managing users where you will increase your security stance as a consequence). I believe it is an excellent framework which you can continually build on and enhance, bringing about even greater benefits to your organisation.”

The annual recertification with URM is a timely reminder and sense check that Sightsavers is still achieving its base line. With regard to the effort involved in achieving and maintaining certification, Andrew was keen to stress, however, that effort to achieve CE is very front-loaded and, provided that you maintain your environment and processes with the necessary tweaks, the annual recertification process should be very straightforward.

> *One of the great things about Cyber Essentials is that it is a targetable standard, so you always know exactly where you are.*
>
> Andrew Blackburn
> Information Security Manager at Sightsavers

For more information on URM Consulting Services:

T: 0118 206 5410
E: info@urmconsulting.com
W: https://www.urmconsulting.com

For more information on Sightsavers:

T: 01444 446 600
E: info@sightsavers.org
W: https://www.sightsavers.org

CYBER ESSENTIALS CERTIFIED

URM Sightsavers