San-iT

CyberSmart

Cyber security

Is your business safe from cyber attacks?

san-it.co.uk

Introductions

Matt Simmons

Technical Director at San-iT Ltd

Adam Footy

Senior Channel Account Manager at CyberSmart

San-iT and CyberSmart

- Work together to help clients become more compliant and cyber secure
- Access to training
- Help to provide IASME certification
- Help to provide the perpetual Governance around Cyber Essentials

Cyber security

Impact of COVID-19 on digital working cyber security

The cyber threat landscape

Are businesses prepared for the new cyber security?

How can we be sure around these risks?

Impact of COVID-19 on digital working and cyber security

- Increased working from home
- Lack of “Cyber-safe” remote working environments
- Many more virtual meetings
- Greater exposure to risk outside of the office
- The average cost of a data breach resulting from remote working can be as much as £115,000

The cyber threat landscape

- Malicious employees
- Cybercriminals
- The activities of hacktivists
- Script kiddies (‘junior’ hackers with less technical skills)

But why the sudden spikes?

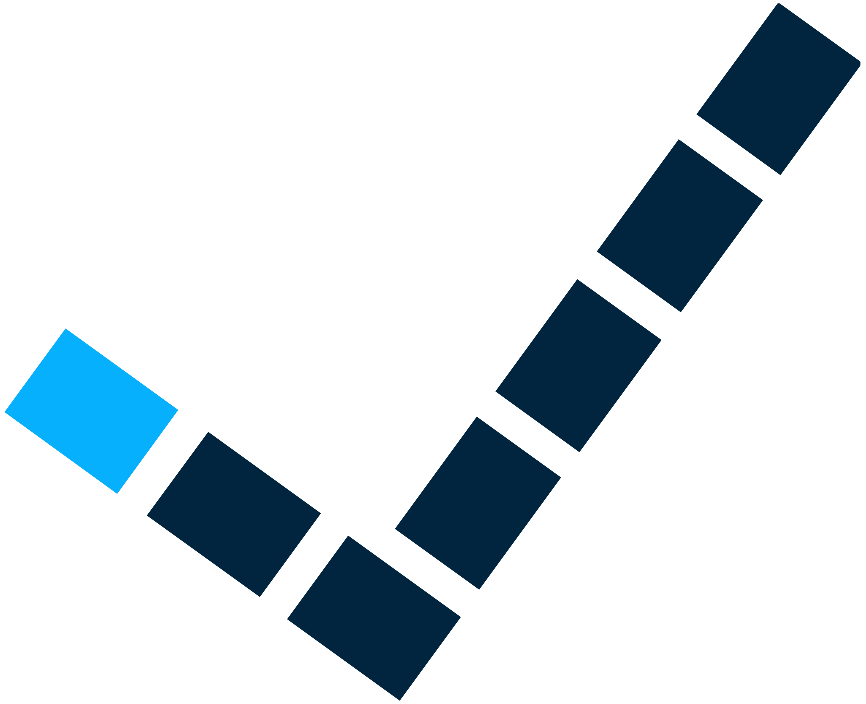
- The increase in, especially SMBs, the use of BYOD approaches instead of business owned and enabled
- Home networks are much easier to attack
- Human error is another issue of concern
- Hackers are upping their game

So are businesses prepared for the new risks?

- Antivirus protection
- Cybersecurity awareness programme
- Phishing awareness programme
- Phishing awareness
- Home network security
- VPNs in use
- IT weak spots
- Review your risk exposure
- Business continuity plans
- Staff awareness and training plans

Quick practical low-cost wins?

- MFA
- Password manager / vault
- Password policies
- Anti-virus managed for a whole business
- Secure connections to office
- Policies for cyber and continuity
- Send staff on training webinars



San-iT CyberSmart

How can you be sure around these risks?

CyberSmart credentials

- Secure by design: Independently tested in NCSC proving grounds and ISO 27001 certified
- Built for scale: Network of MSPs and corporate partners
- Widely adopted: from Government to single-person SMEs
- Cyber Security Startup of the Year 2019
- CompTIA Innovative Vendor of the Year 2020

Cyber Security Awards
Winner 2019

Evening Standard
Progress 1000

IASME Consortium®

gov.scot

CYBER ESSENTIALS
CERTIFIED

CYBER ESSENTIALS
CERTIFIED PLUS

HM Government

Cyber Accelerator Alumni
in association with
National Cyber Security Centre

Information Security Management
ISO 27001
Certified

What Do We Do?

CyberSmart offers you a **simple, step-by-step journey to securing a business**.

We're built for SMEs so there's no cyber expertise needed.

What is Cyber Essentials

- A Government and NCSC collaboration
- Thought to be **80%** effective at the point of creation
- Proven by the University of Lancaster to be **99.3%** effective
- Deliberately aimed at small businesses
- Mandated to Government and Local Government
- Self Assessment Questionnaire
- Firewall, Secure Configuration, Malware Protection, User Access Control and Patch Management

Why is Cyber Essentials

- Protect you against common cyber attacks
- GDPR Compliance
- It shows your customers sand suppliers that you take cyber security seriously
- Free cyber security insurance

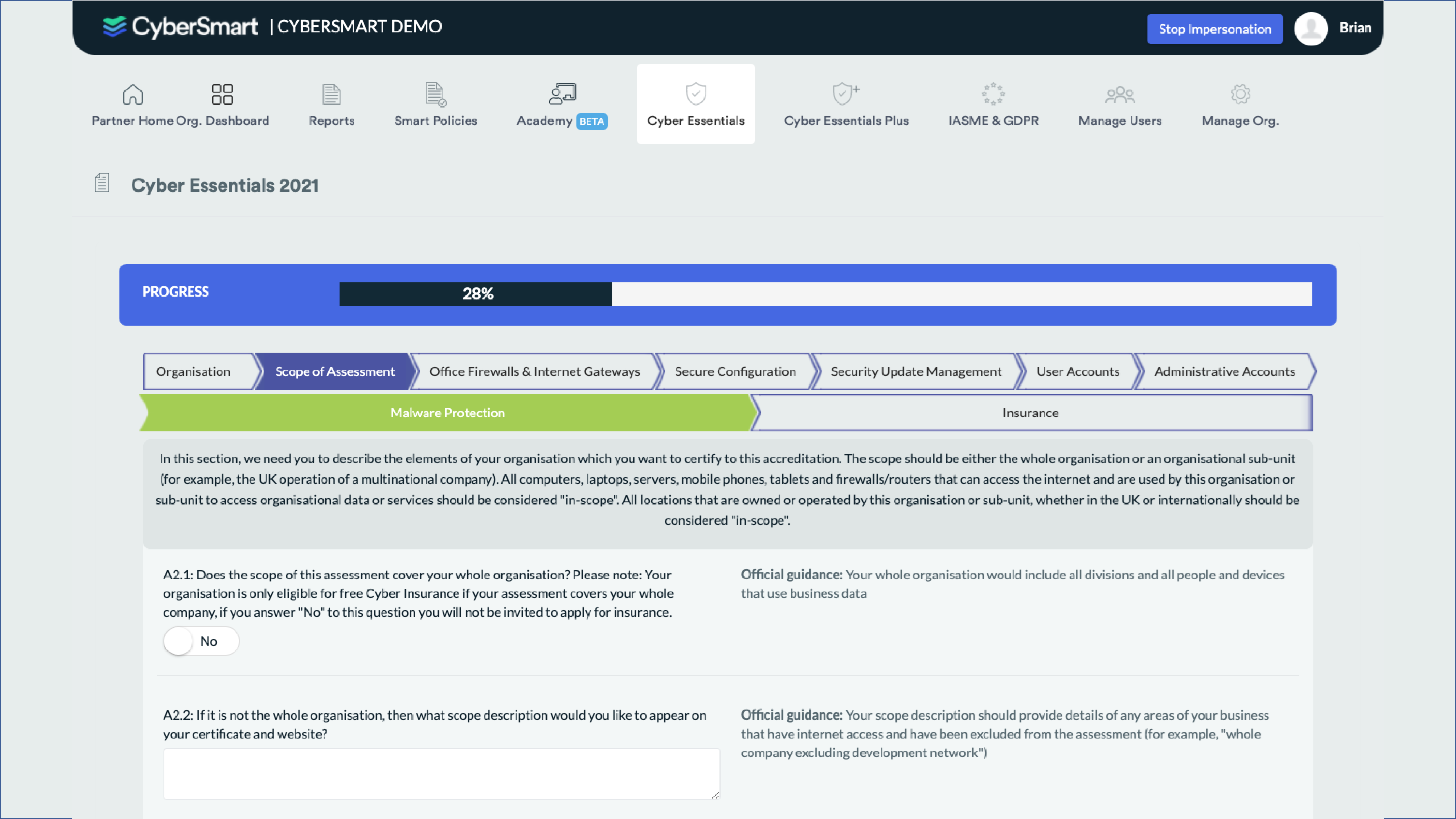
The five security controls

- Firewall
- Secure configuration
- Malware protection
- User access control
- Patch management

CYBER ESSENTIALS

How it works **with** CyberSmart

- Guided questionnaire
- Single pane of glass dashboard
- Everyday security, not one day security
- Fail-free environment
- Questionnaire scrutinised internally, not with IASME
- No time restraints to resubmit



Cyber Essentials 2021

In this section, we need you to describe the elements of your organisation which you want to certify to this accreditation. The scope should be either the whole organisation or an organisational sub-unit (for example, the UK operation of a multinational company). All computers, laptops, servers, mobile phones, tablets and firewalls/routers that can access the internet and are used by this organisation or sub-unit to access organisational data or services should be considered "in-scope". All locations that are owned or operated by this organisation or sub-unit, whether in the UK or internationally should be considered "in-scope".

A2.1: Does the scope of this assessment cover your whole organisation? Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to apply for insurance.

○ No

Official guidance: Your whole organisation would include all divisions and all people and devices that use business data

A2.2: If it is not the whole organisation, then what scope description would you like to appear on your certificate and website?

Official guidance: Your scope description should provide details of any areas of your business that have internet access and have been excluded from the assessment (for example, "whole company excluding development network")

What is Cyber Essentials Plus?

- Follows the exact same framework: Firewall, Secure Configuration, Malware Protection, User Access Control and Patch Management
- Information is obtained in a vastly different way
- Required an independent auditor
- Held in a higher regard over Cyber Essentials
- In huge demand

CYBER
ESSENTIALS PLUS

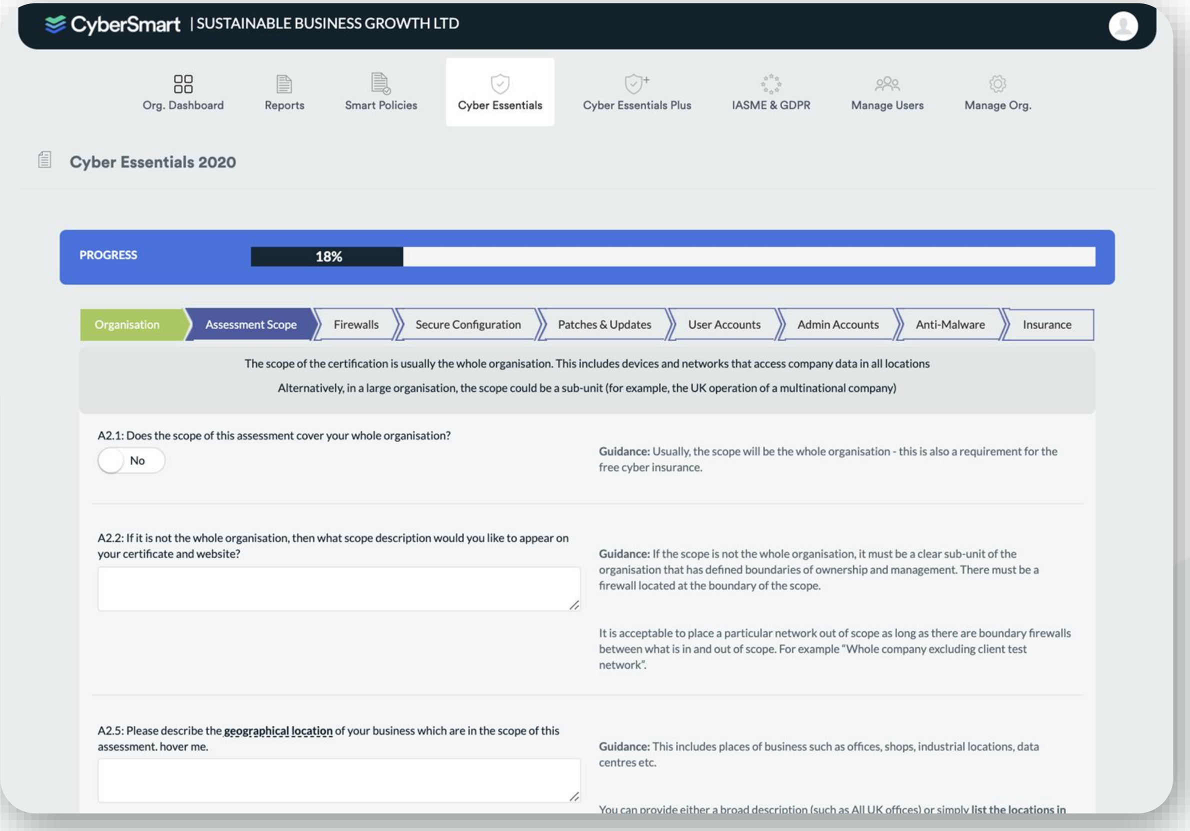
How it works **with** CyberSmart

- Reports scrutinised internally, not with IASME
- Rescans included
- Completely fail free environment
- 100% remote
- On site if preferred
- No time restraints to resubmit

Changes

- NHS now required to have Cyber Essentials as part of the Data Security and Protection Toolkit (DSPT)
- From 2022, NHS will be required to have Cyber Essentials Plus
- Education now required to have Cyber Essentials
- Education required to have Cyber Essentials Plus from 2022

Compliance every day, not one day:



Cyber Essentials 2020

PROGRESS 18%

Organisation | Assessment Scope | Firewalls | Secure Configuration | Patches & Updates | User Accounts | Admin Accounts | Anti-Malware | Insurance

The scope of the certification is usually the whole organisation. This includes devices and networks that access company data in all locations

Alternatively, in a large organisation, the scope could be a sub-unit (for example, the UK operation of a multinational company)

A2.1: Does the scope of this assessment cover your whole organisation?

○ No

Guidance: Usually, the scope will be the whole organisation - this is also a requirement for the free cyber insurance.

A2.2: If it is not the whole organisation, then what scope description would you like to appear on your certificate and website?

Guidance: If the scope is not the whole organisation, it must be a clear sub-unit of the organisation that has defined boundaries of ownership and management. There must be a firewall located at the boundary of the scope.

It is acceptable to place a particular network out of scope as long as there are boundary firewalls between what is in and out of scope. For example "Whole company excluding client test network".

A2.5: Please describe the geographical location of your business which are in the scope of this assessment. hover me.

Guidance: This includes places of business such as offices, shops, industrial locations, data centres etc.

You can provide either a broad description (such as All UK offices) or simply **list the locations in**

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

IASME GDPR

San-iT

CyberSmart

Thank you

Any questions?