IASME Consortium ®

Cyber Essentials

Jamie Randall

Chief Technology Officer, IASME Consortium

About the IASME Consortium

- UK Government funded project to develop “an alternative to ISO27001 for SMEs”
- Resulted in the IASME governance standard
- Company formed on completion of project (5 years ago)
- 2013 – UK Government endorsed IASME as best cyber security governance standard for SMEs
- IASME invited to help write the Cyber Essentials standard for the UK Government – representing SMEs

Current situation

- Extremely low levels of Cyber Security in many SMEs (and larger companies)
- General assumption that it is higher
- ‘Flow down’ of security requirements in supply chains not working
- Key vulnerabilities for whole supply chain

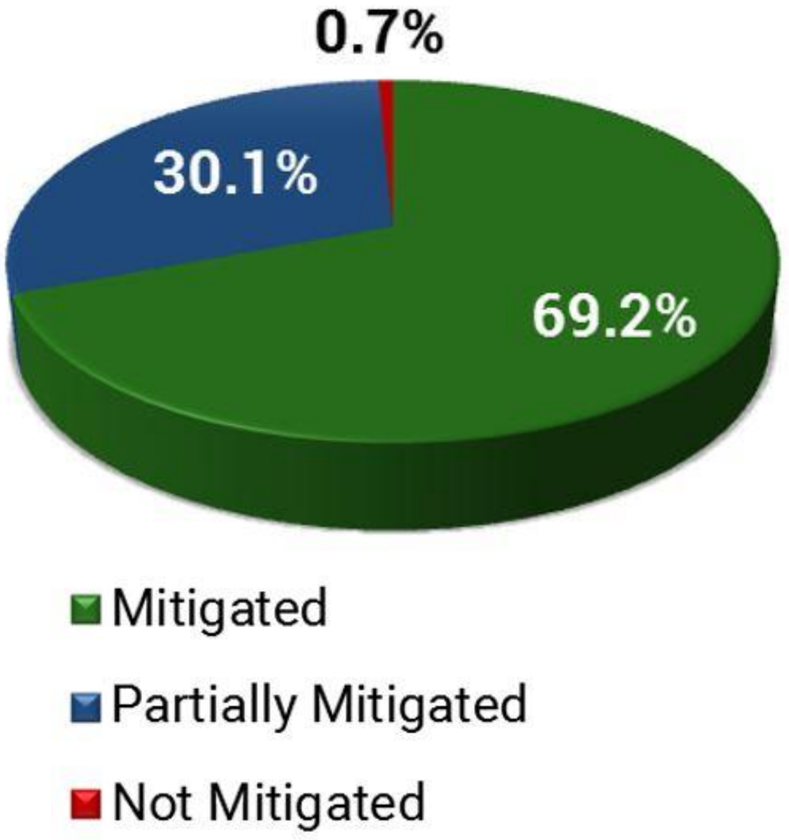
Background to Cyber Essentials

- Frustration from UK Government – many breaches due to lack of simple controls
- Review of breaches over 4 years resulted in identification of 5 key technical controls
- IASME worked with UK Government to write Cyber Essentials Requirements
- Cyber Essentials scheme aims at getting all companies to implement these 5 most important controls

Why bother?

- Increasingly mandated in government contracts – including supply chain
  - Mandated in UK Government contracts since 1st October 2014
  - MOD
  - Large company supply chains
- It works…

Lancaster University Research



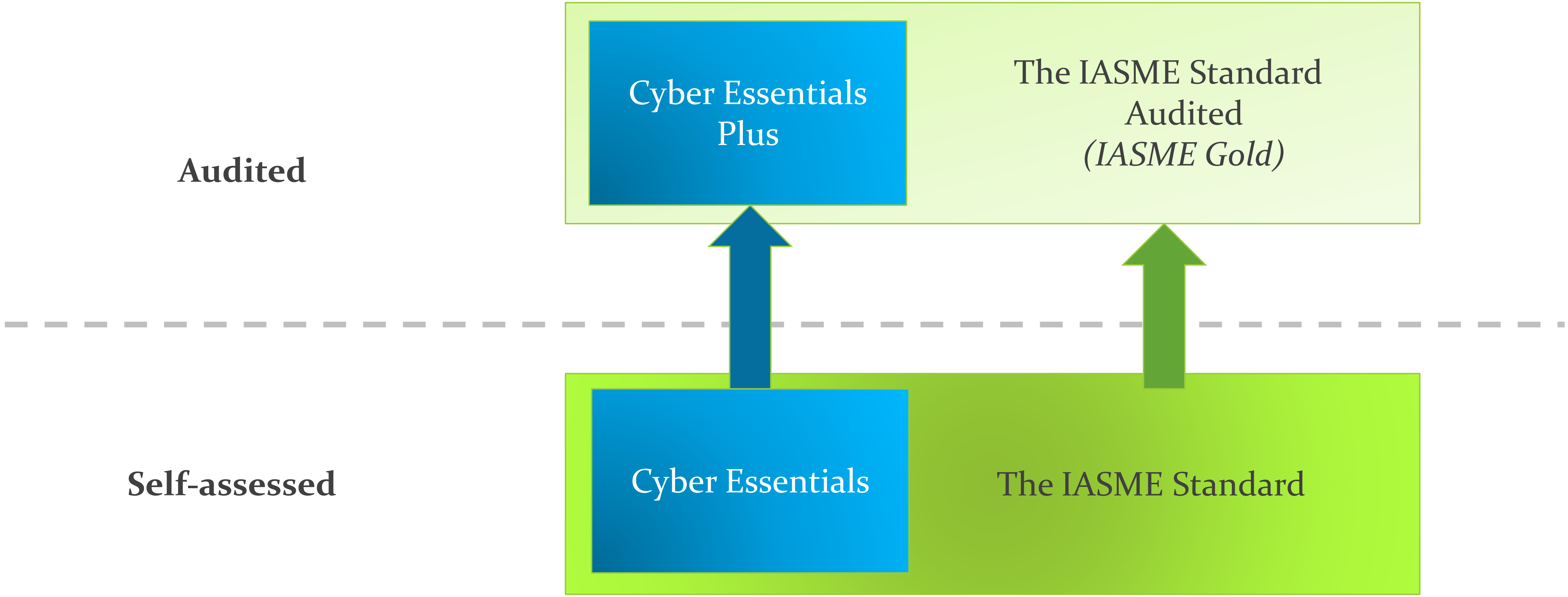
“without the Cyber Essentials controls none of the attacks assessed were mitigated on any network

This, more than anything else should be understood by SMEs, **taking no action to combat cyber threats simply isn’t an option.**

With the CE tools, more than 99% of the vulnerabilities in SMEs interviewed were mitigated.”

* *Cyber Essentials Aggregated Vulnerability Mitigation Results*
Lancaster University, 2015

IASME & Cyber Essentials Standards



Audited

Cyber Essentials Plus

The IASME Standard Audited *(IASME Gold)*

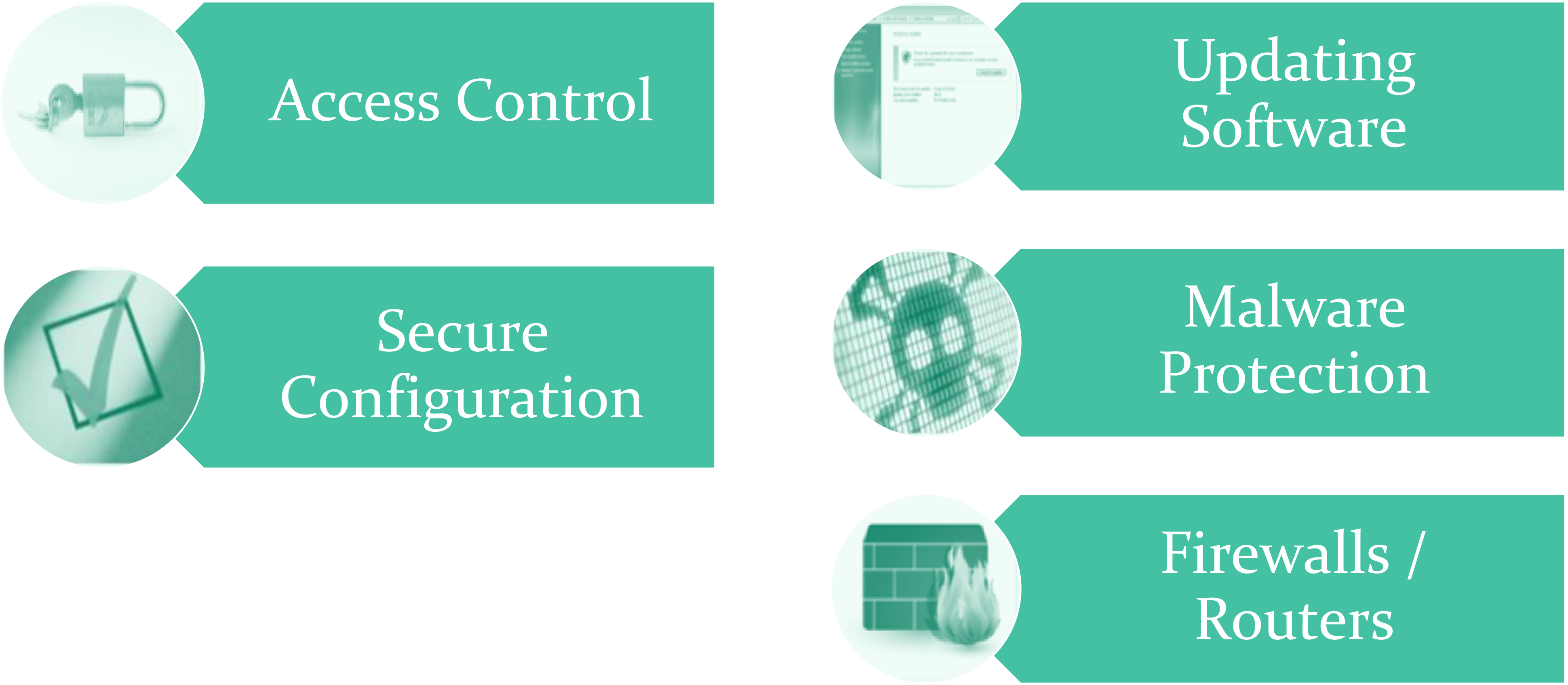
Self-assessed

Cyber Essentials

The IASME Standard

Visit www.iasme.co.uk or call 03300 882 752

Cyber Essentials



Access Control

Secure Configuration

Updating Software

Malware Protection

Firewalls / Routers

Access Control

To prevent unhappy staff or external cyber criminals making system changes

- Do not work using an administrator account day-to-day
- Use strong admin password
- Do you have a list of (and process for) people in your organisation with admin privileges?
- No users with same username and password

Secure Configuration

Locking any open doors which are not required

- Close accounts which are not used
- Remove software you don't need
- Change all default admin passwords to a strong password
- Disable 'auto run' features

Keeping software updated

To prevent cyber criminals using the mistakes they find in software as a way to get into your system

- Correct licences for your software
- All software supported (no Windows XP/2003!)
- Set to update automatically
- Receiving security patches

Anti-malware

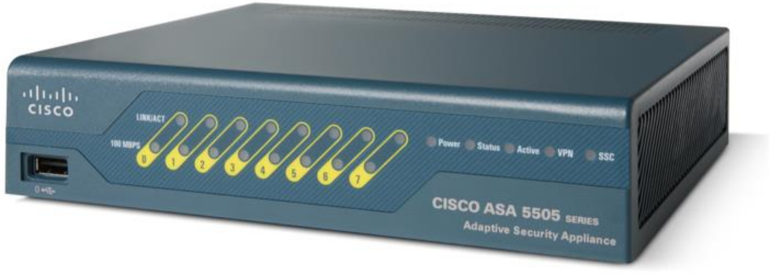
To spot and immobilise viruses before they have a chance to do anything.

- Anti-virus on ALL computers
- Set to update itself automatically
- Set to 'scan on access'
- Warn you about malicious websites

Firewalls/routers

Protection between your computers and the internet

- Needed on
  - Office
  - Devices
  - Home offices
- Change default password to a strong one
- Prevent your network being exposed to the internet
- Authentication to access internal services from internet



Cyber Essentials

- Basic level Cyber Essentials
  - Self assessment signed off at Board Level and assessed by independent organisation.
- Cyber Essentials PLUS
  - internal and external vulnerability test & onsite technical audit

Two sides of securing a company

- Technical security
  - Cyber Essentials
- Governance and understanding of Risk
  - IASME standard
  - ISO27001

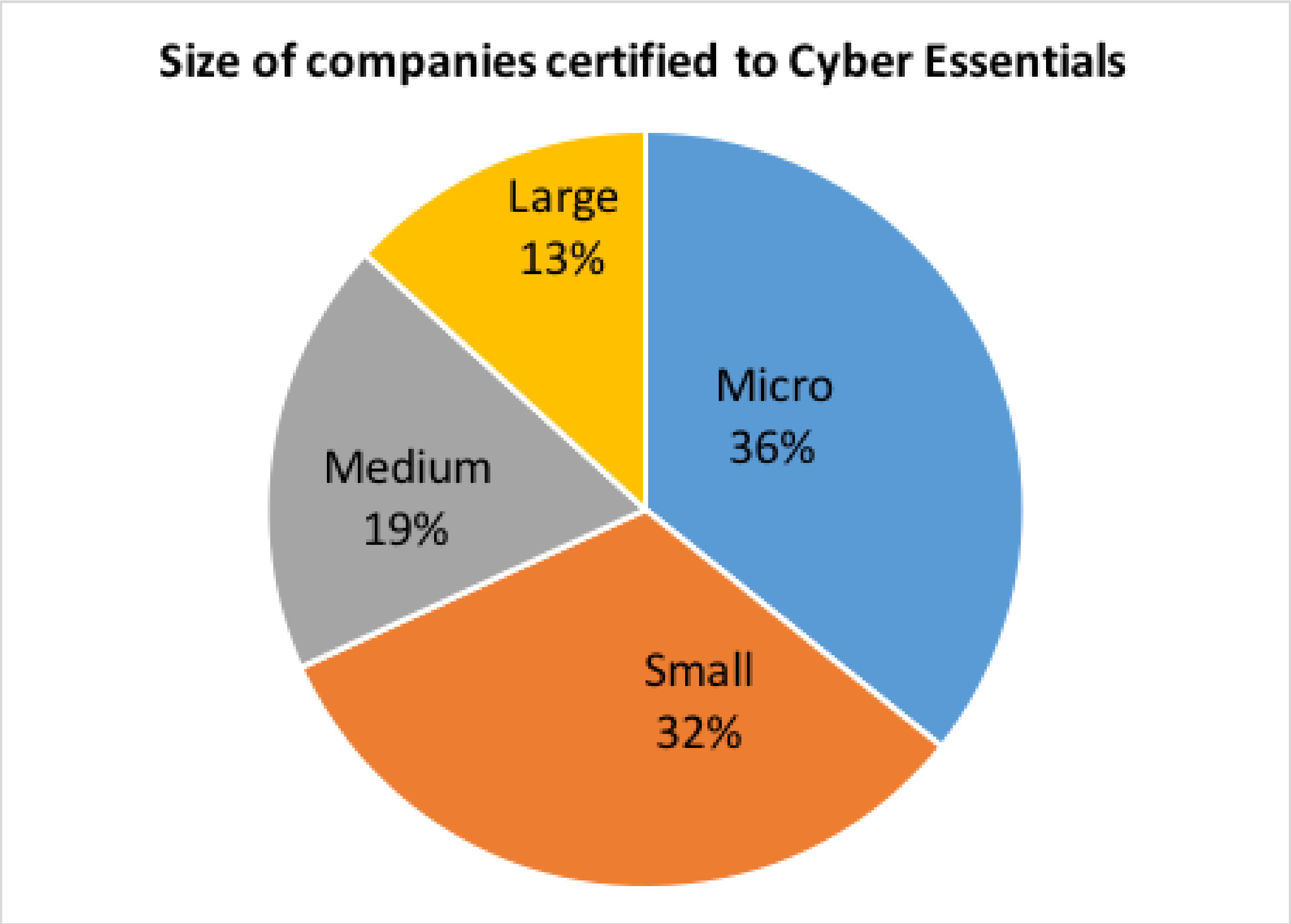
IASME adds further categories of security controls to those of Cyber Essentials

Cyber Essentials	IASME
Business Scope	Public Internet Data Storage
Access Control	Security Management
Secure Configuration	Assessing the Risk
Software Patching	Policy & Compliance
Malware & Network Intrusion	Data Protection
Protection between your systems and the internet	Key Information Assets
	People
	Physical and Environmental Protection
	Access Control
	Operations and Management
	Monitoring
	Backup and restore
	Incident Management
	Business Continuity
78 Questions	**160 Questions**

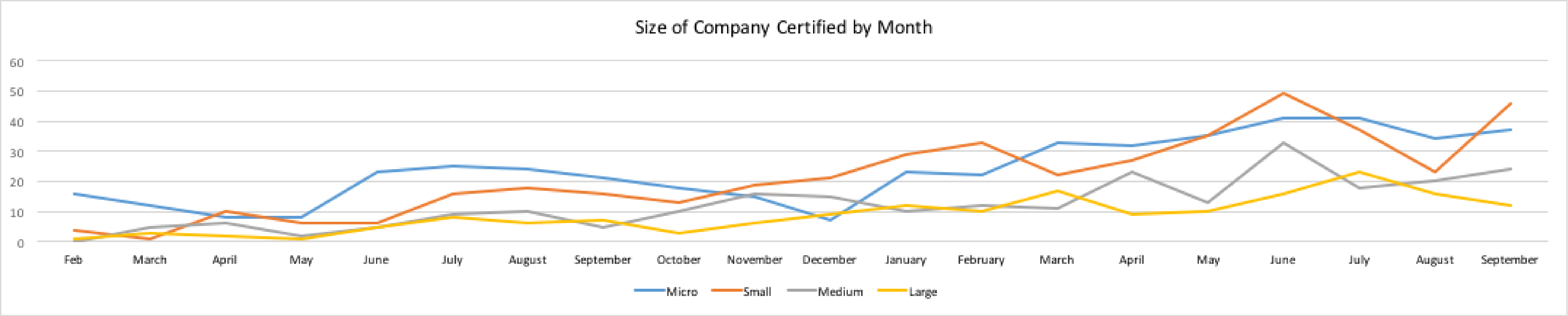
What have we learnt?

Take-up of Cyber Essentials

- Launched over 2 years ago – take up is accelerating
- Currently being considered by a number of countries to be mandatory.


Size of companies certified to Cyber Essentials
Large
13%
Micro
36%
Medium
19%
Small
32%

Link to HMG tenders



Biggest reason for failure in UK

- Unsupported software (usually Windows XP or Server 2003)

Summary

- A few small technical changes will prevent 80% of cyber attacks
- Cyber Essentials is relatively simple and is effective
- IASME governance certification offers a next step towards information assurance

IASME Consortium ®

Thank you