CyCOS

Cyber Security Communities of Support

University of Nottingham
UK | CHINA | MALAYSIA

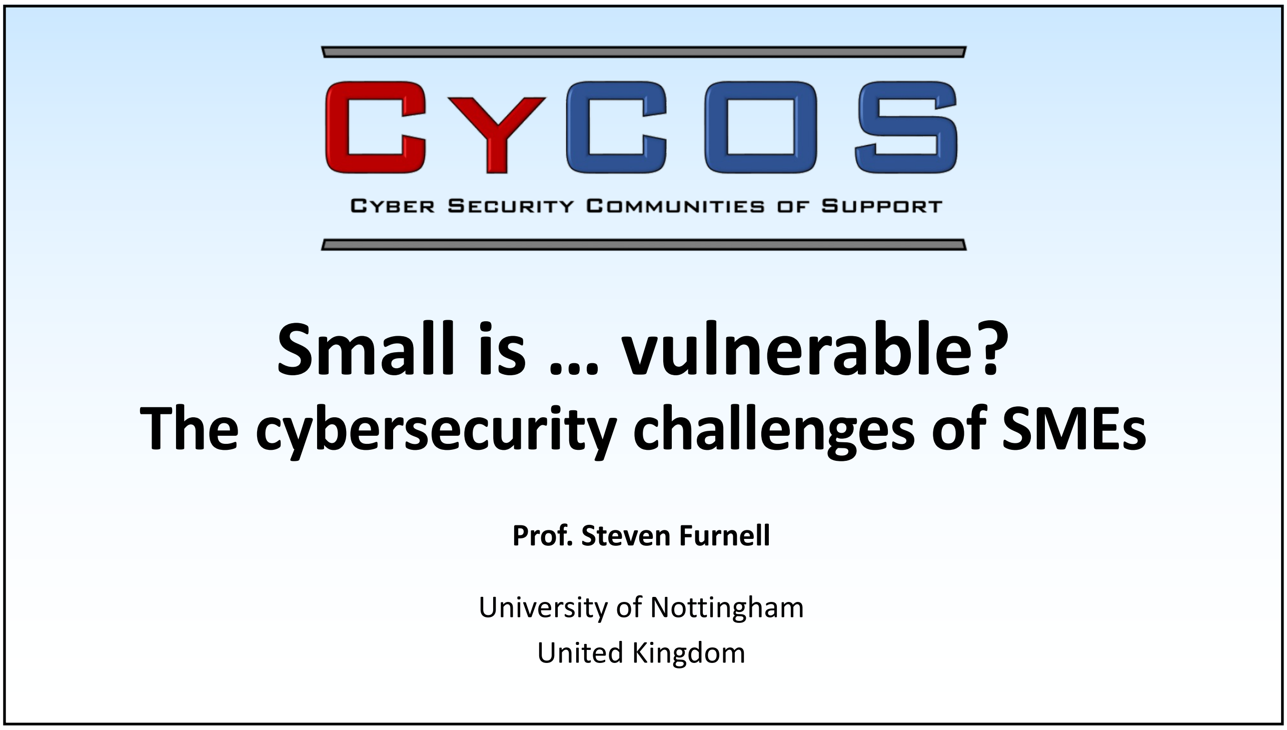
Queen Mary
University of London

University of Kent

UKRI
Engineering and Physical Sciences Research Council

RISCS
Research Institute for Sociotechnical Cyber Security

1



CyCOS

Cyber Security Communities of Support

Small is … vulnerable?

The cybersecurity challenges of SMEs

Prof. Steven Furnell

University of Nottingham
United Kingdom

2

Introduction

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

- Cybersecurity is an ongoing challenge for all organisations
  - technology usage and network connectivity are fundamental foundations of modern businesses operation
- Small and Medium Enterprises (SMEs) are no exception
  - play a crucial role in the economic context
  - often a key element of the supply ecosystem for larger organisations
- Cybersecurity challenge is likely to be more pronounced
  - availability of related knowledge, skills and budgets is typically lower
- Does not lessen the risk
  - despite their size SMEs face many of the same threats as their larger counterparts

3

3

A bit about me ☺

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

- Professor of Cyber Security
- Author of over 360 refereed papers
- Editor of Information and Computer Security
- Board member of the Chartered Institute of Information Security
- Working with the UK Cyber Security Council
- UK representative to IFIP TC11
- *Contributor to DSIT Cyber Security Breaches Survey 2021 and 2023*

4

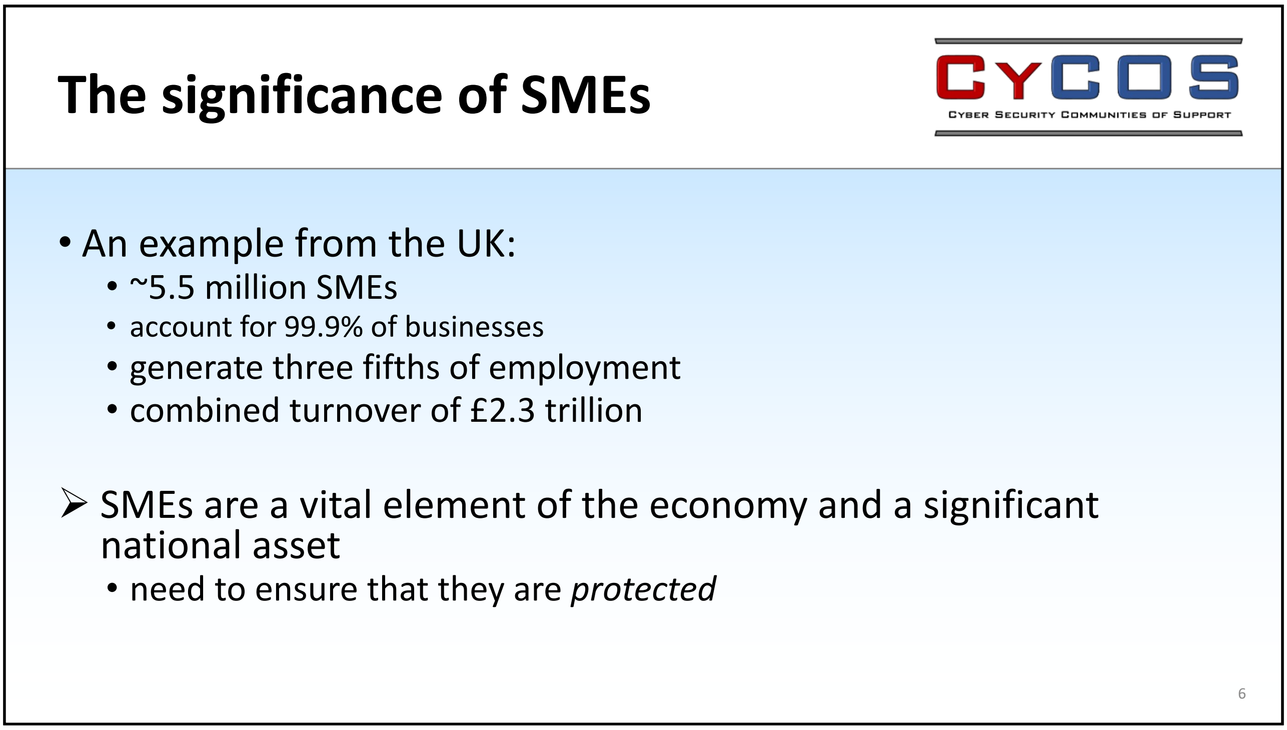
4

Where I'm from

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

5

5



The significance of SMEs

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

- An example from the UK:
  - ~5.5 million SMEs
  - account for 99.9% of businesses
  - generate three fifths of employment
  - combined turnover of £2.3 trillion

➢ SMEs are a vital element of the economy and a significant national asset
  - need to ensure that they are *protected*

6

6

SMEs and cyber security

- Small businesses are typically not well placed in terms of cyber expertise and capability
- Many (~50%*) outsource their security
  - still requires knowledge of *where* to look and what to look *for*
- Others may be reliant on limited in-house knowledge
- Others are potentially overlooking things entirely

**Cyber Security Breaches Survey 2023*

A lack of skills?

Cyber security skills in the UK labour market 2023

Findings report

Steve Coutinho, Alex Bollen, Claire Weil, Chloe Sheerin, Dejon Silvera, Ipsos
Sam Donaldson, Jade Rosborough, Perspective Economics

- 50% of businesses have a **basic skills gap** in relation to technical cyber security (estimated ~739,000 businesses)
  - includes *configuring firewalls*, *detecting and removing malware*, and *choosing secure settings*
- The gap is lower in large businesses (18%)
  - SMEs face the more pronounced problem
- Many SMEs are ill-positioned to address their own needs
  - leaves them exposed and dependent upon further support in the event of incidents, or when making security related decisions (including those around technology adoption and procurement)

My main source …

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

Department for
Science,
Innovation
& Technology

Official Statistics

Cyber security breaches survey 2023

Published 19 April 2023

Contents

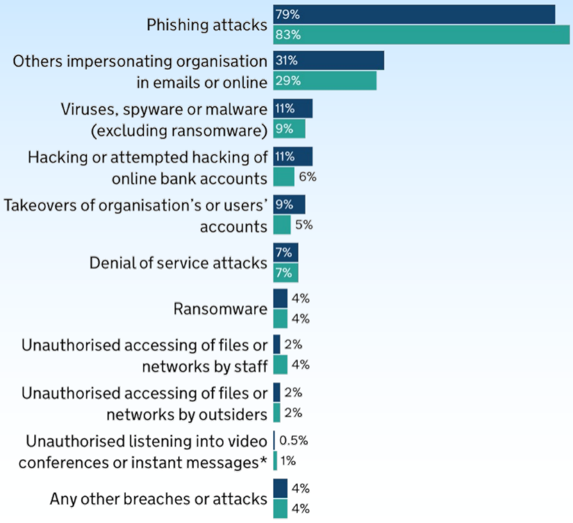
www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

9

9

Breaches and attacks

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

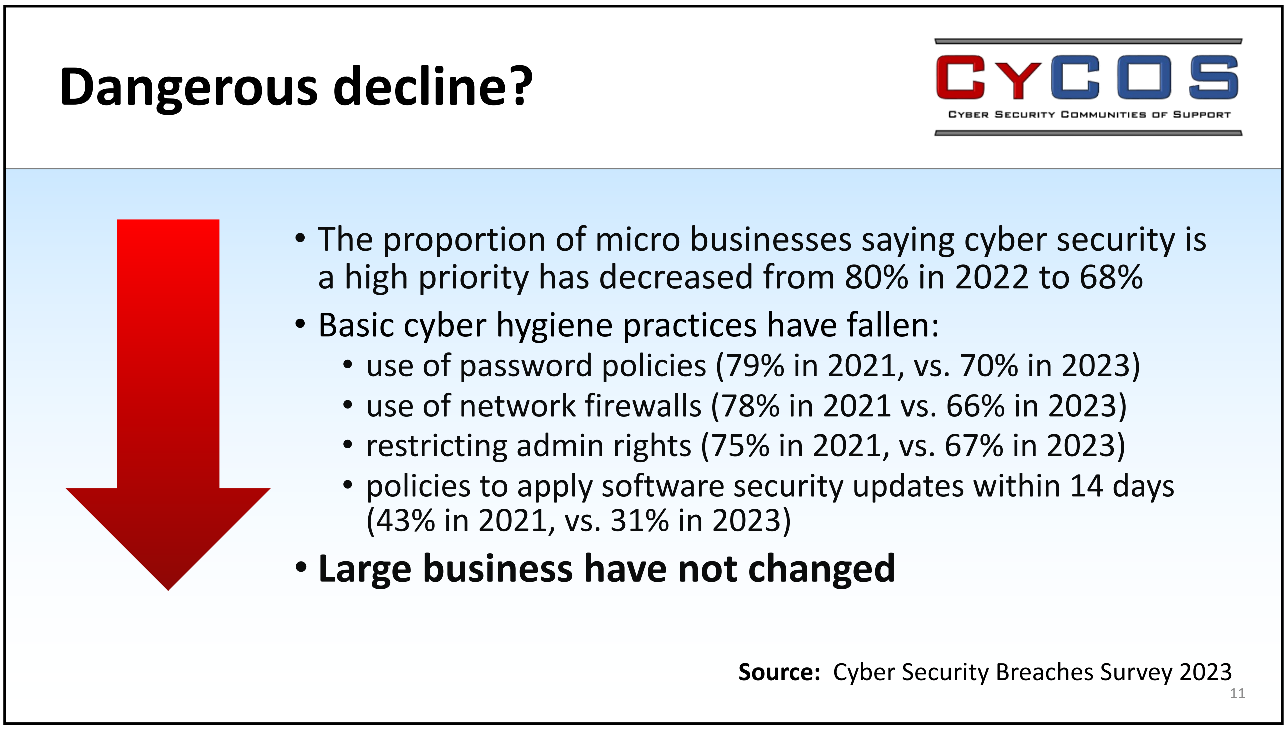


Overall, 32% of businesses and 24% of charities had identified breaches or attacks in the last 12 months

Bases:
887 businesses that identified a breach or attack in the last 12 months; 435 charities

10

10



Dangerous decline?

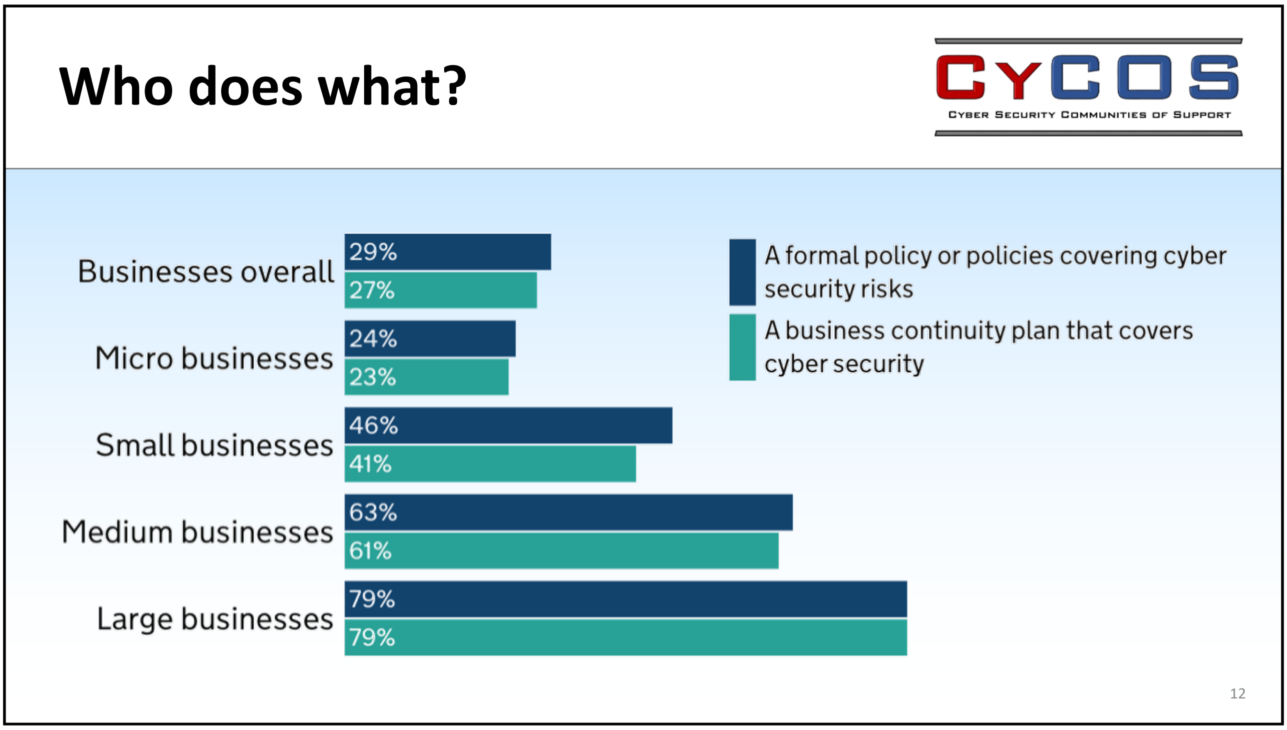
CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

- The proportion of micro businesses saying cyber security is a high priority has decreased from 80% in 2022 to 68%
- Basic cyber hygiene practices have fallen:
  - use of password policies (79% in 2021, vs. 70% in 2023)
  - use of network firewalls (78% in 2021 vs. 66% in 2023)
  - restricting admin rights (75% in 2021, vs. 67% in 2023)
  - policies to apply software security updates within 14 days (43% in 2021, vs. 31% in 2023)
- **Large business have not changed**

Source: Cyber Security Breaches Survey 2023

11

11

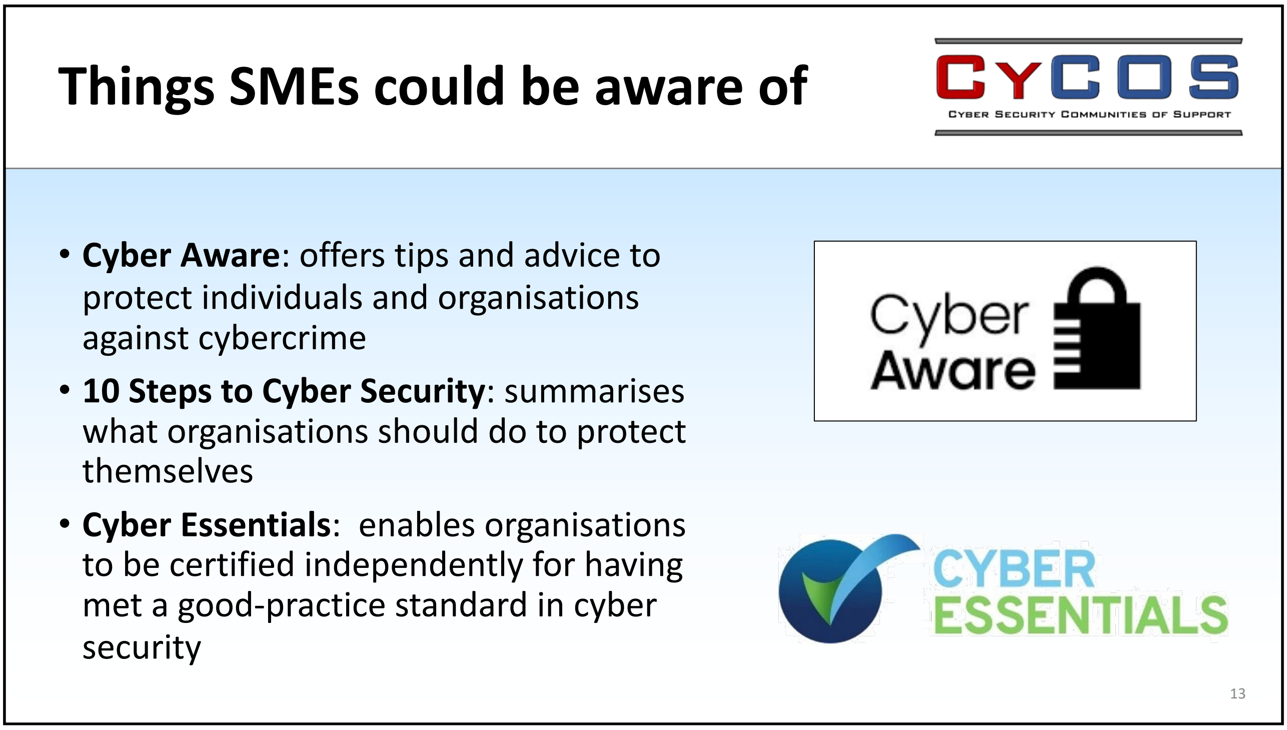


Who does what?

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

12

12



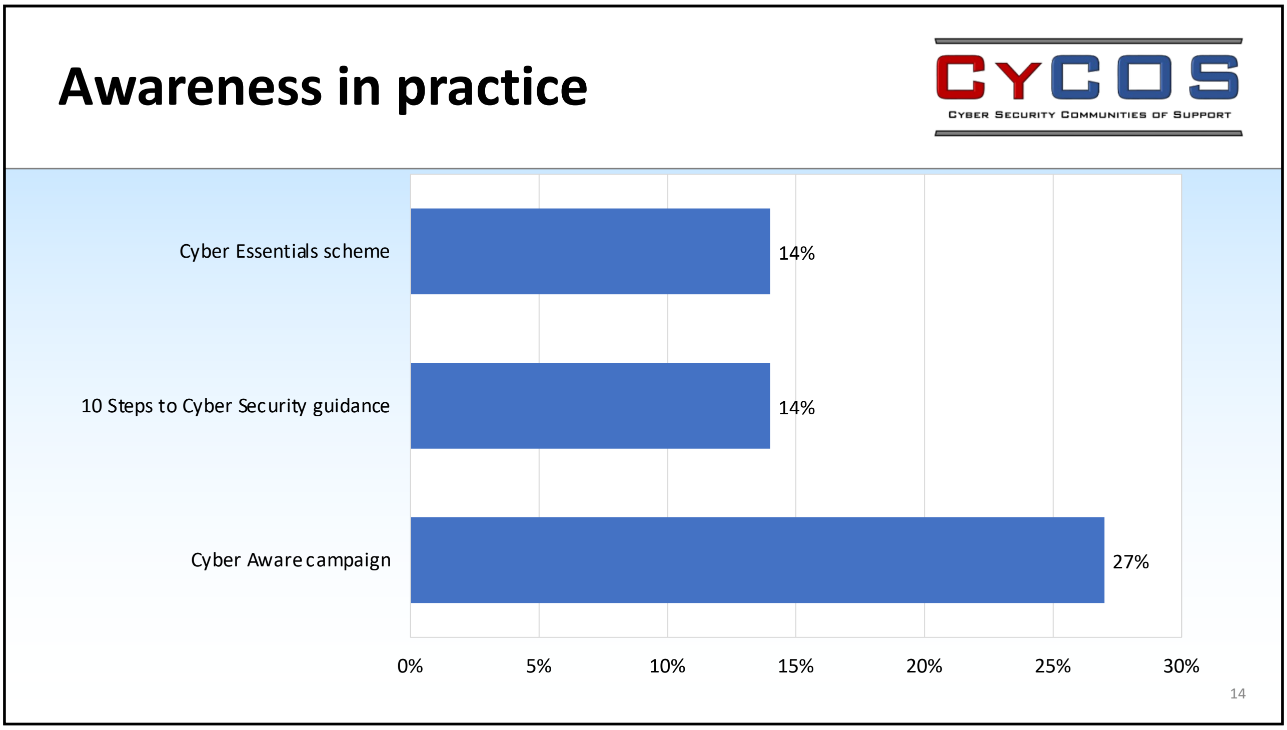
Things SMEs could be aware of

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

- **Cyber Aware**: offers tips and advice to protect individuals and organisations against cybercrime
- **10 Steps to Cyber Security**: summarises what organisations should do to protect themselves
- **Cyber Essentials**: enables organisations to be certified independently for having met a good-practice standard in cyber security

13

13

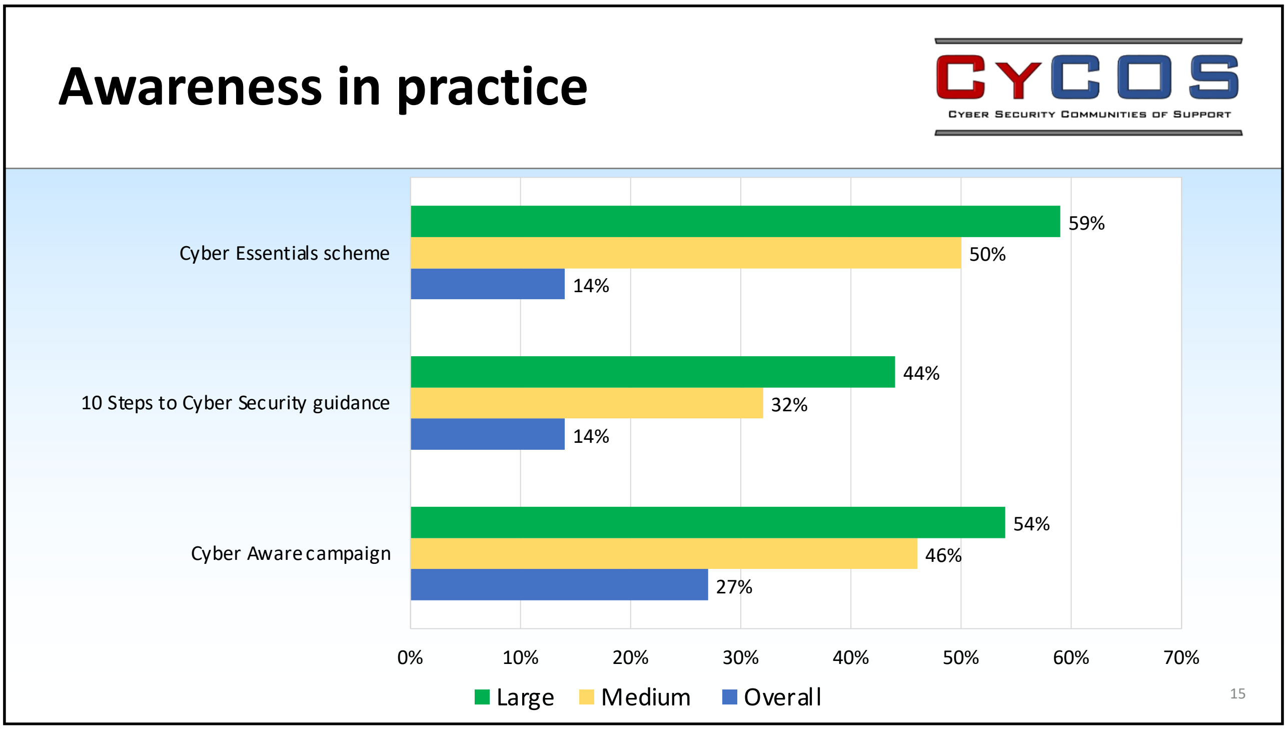


Awareness in practice

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

14

14

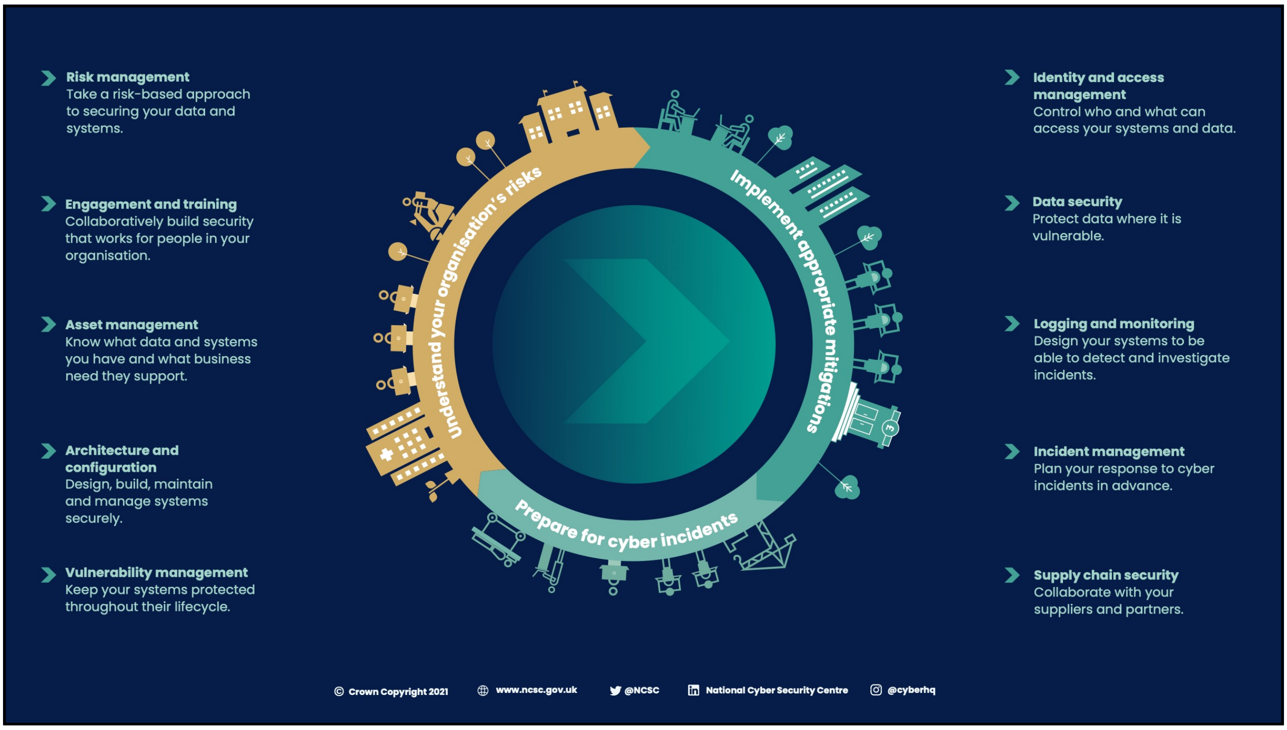


Awareness in practice

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

15

15



Risk management
Take a risk-based approach to securing your data and systems.

Engagement and training
Collaboratively build security that works for people in your organisation.

Asset management
Know what data and systems you have and what business need they support.

Architecture and configuration
Design, build, maintain and manage systems securely.

Vulnerability management
Keep your systems protected throughout their lifecycle.

Understand your organisation's risks
Implement appropriate mitigations
Prepare for cyber incidents

Identity and access management
Control who and what can access your systems and data.

Data security
Protect data where it is vulnerable.

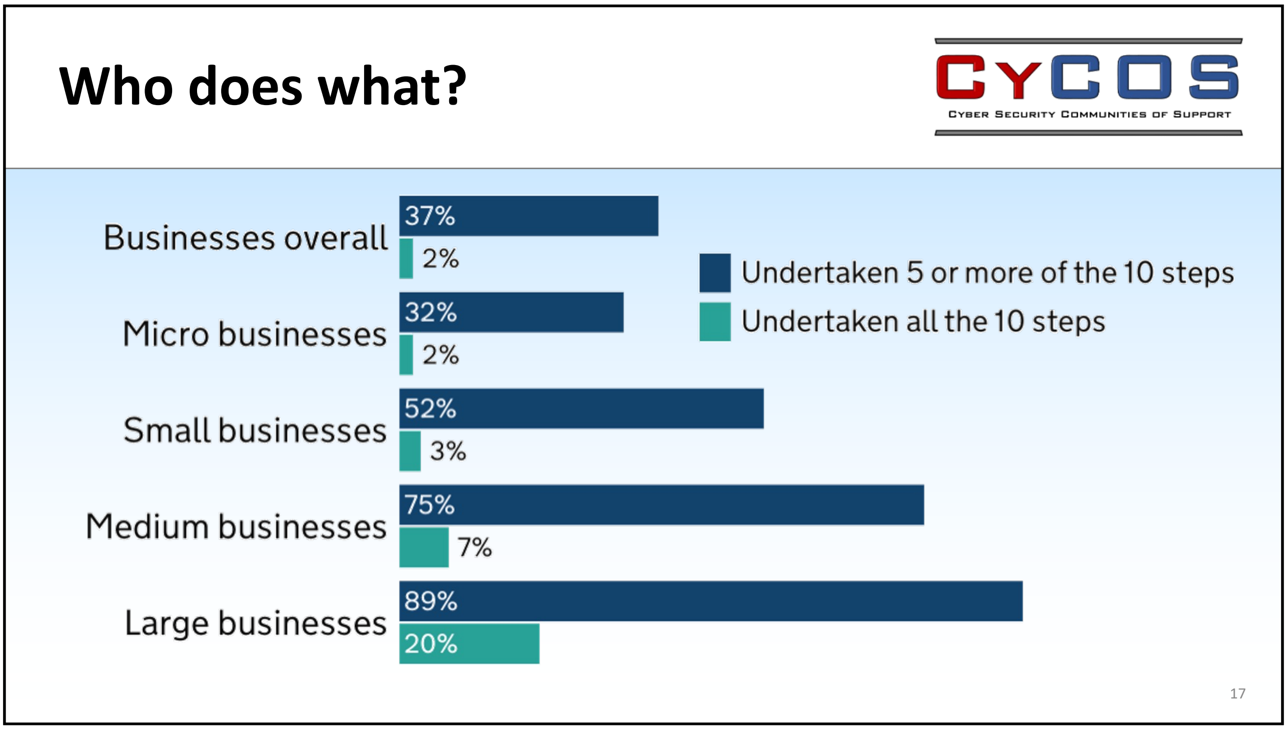
Logging and monitoring
Design your systems to be able to detect and investigate incidents.

Incident management
Plan your response to cyber incidents in advance.

Supply chain security
Collaborate with your suppliers and partners.

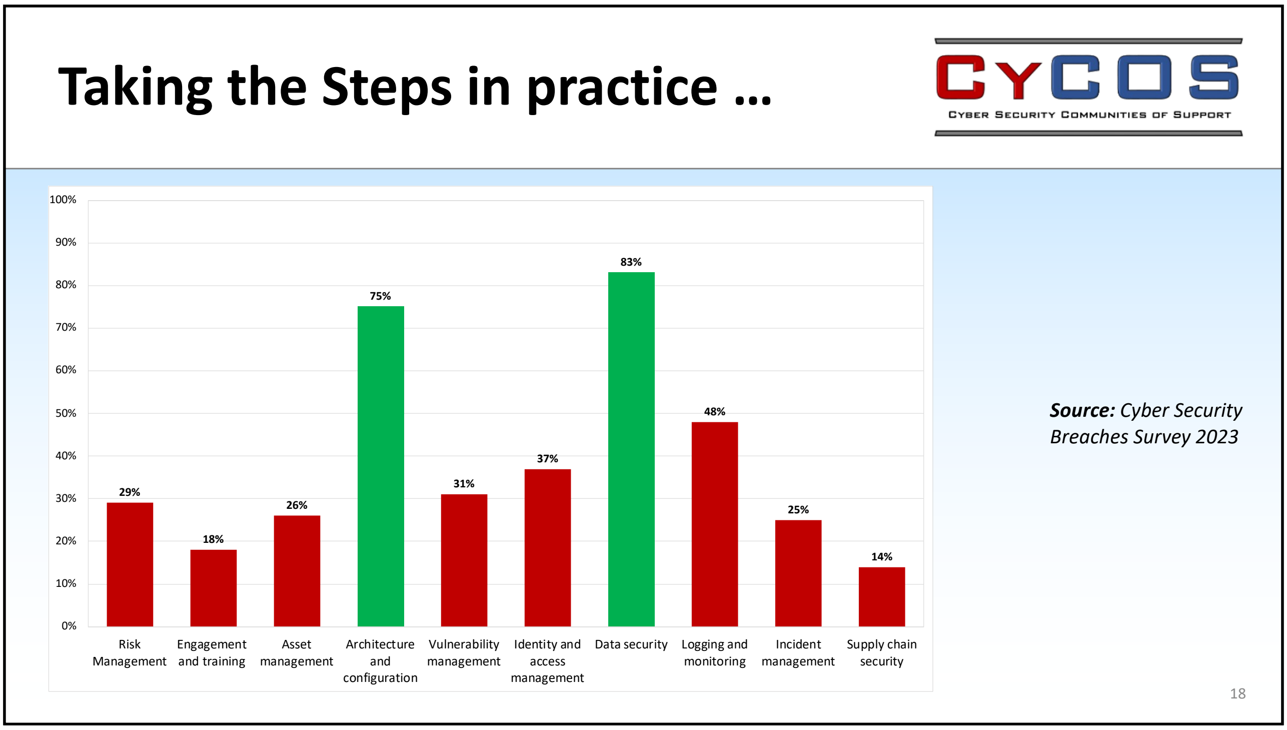
www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

16



Who does what?

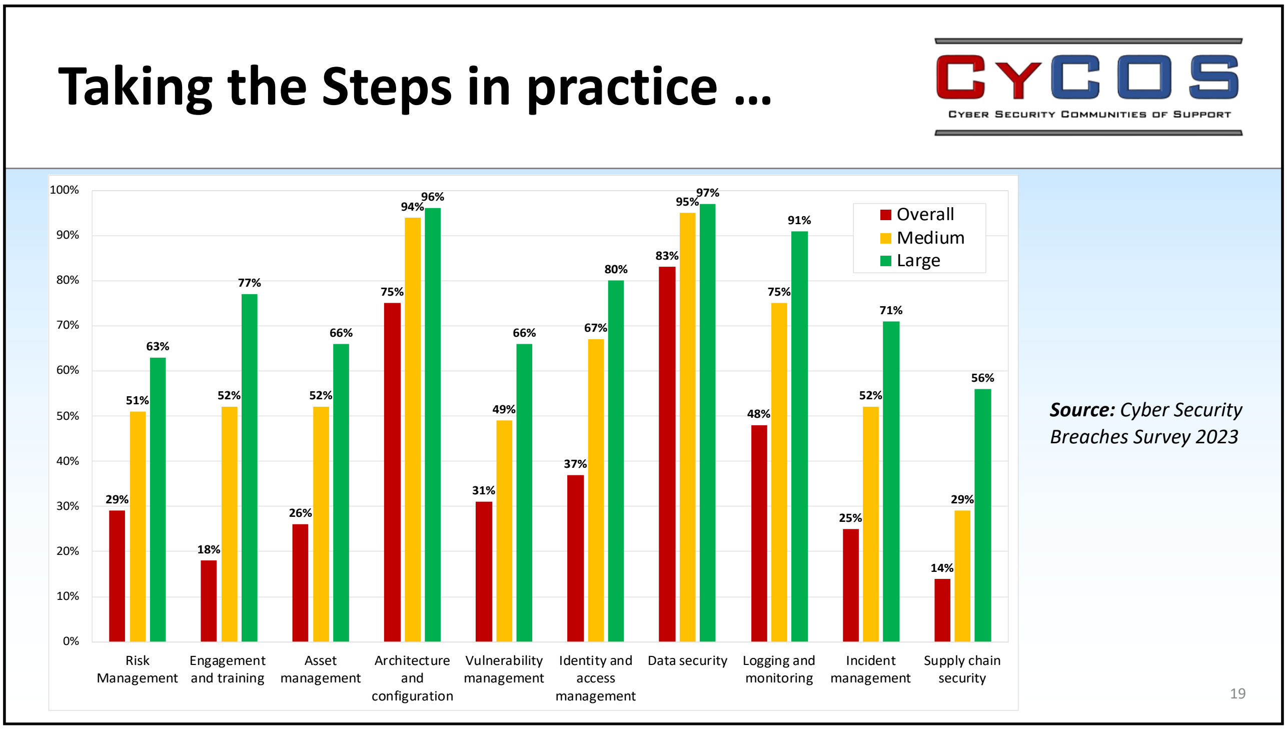
17



Taking the Steps in practice …

Source: *Cyber Security Breaches Survey 2023*

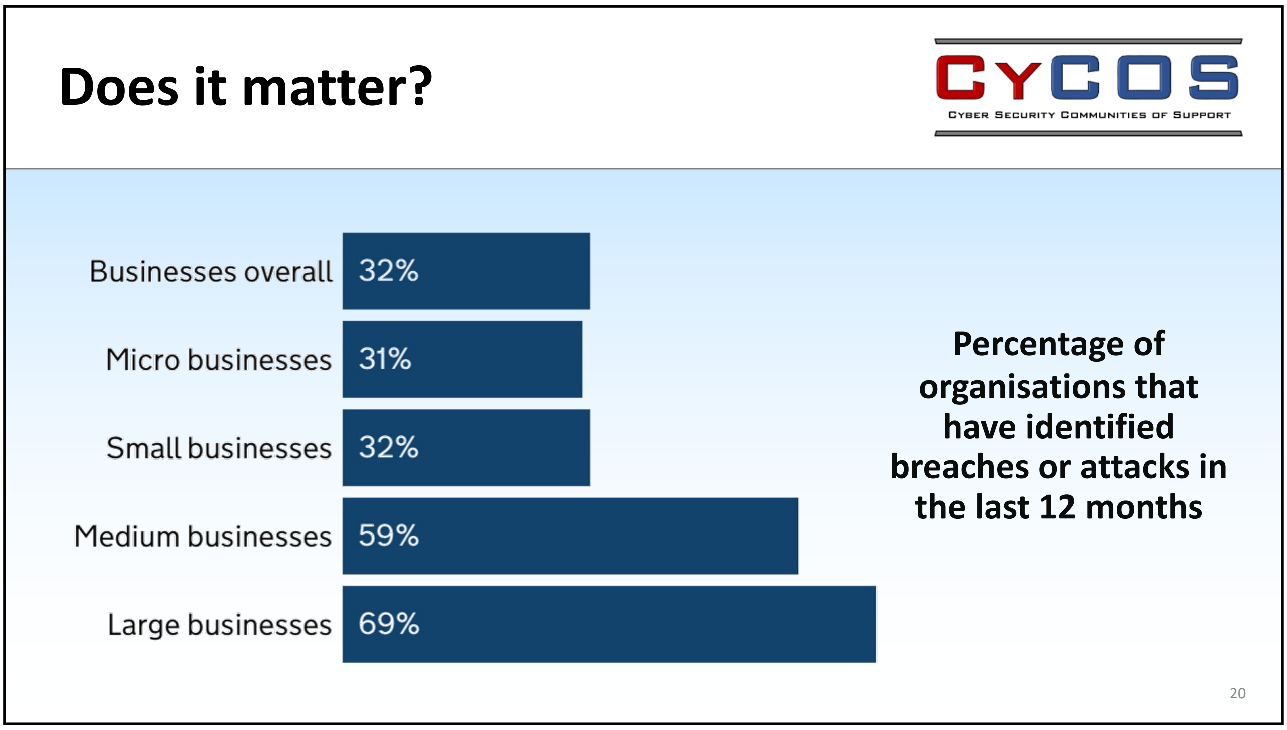
18



Taking the Steps in practice …

Source: *Cyber Security Breaches Survey 2023*

19

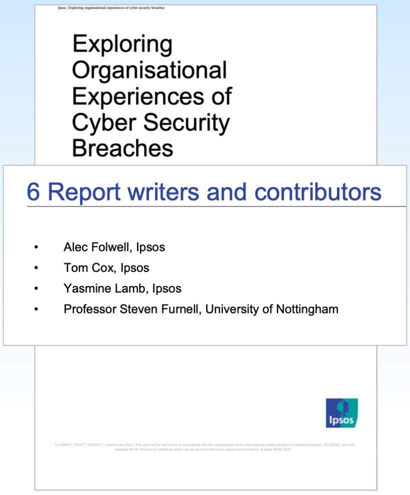


Does it matter?

Percentage of organisations that have identified breaches or attacks in the last 12 months

20

Digging deeper



Ipsos | Exploring organisational experiences of cyber security breaches

Exploring Organisational Experiences of Cyber Security Breaches

6 Report writers and contributors

- Alec Folwell, Ipsos
- Tom Cox, Ipsos
- Yasmine Lamb, Ipsos
- Professor Steven Furnell, University of Nottingham

21-094613 | DRAFT VERION 1 | Internal Use Only | This work will be carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with theIpsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Ipsos MORI 2022

- Undertaken from 23 February to 21 March 2022
- Ten organisations that have collectively experienced a variety of types breach in the last three years
- Qualitative interviews conducted via Microsoft Teams
- At least two employees per organisation and conducted separately:
  - typically someone in an IT or cyber security role who dealt with the breach
  - another member of staff who was directly impacted by it

21

Case study coverage

- **Types of organisation:**
  - 1 micro
  - 2 small
  - 3 medium
  - 4 large

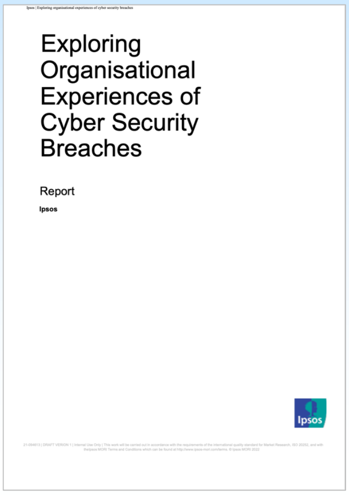
- **Types of breach:**
  - 3 Denial-of-Service
  - 3 Ransomware
  - 3 Spear Phishing
  - 1 Smishing

- **Types of impact:**
  - 10 financial
  - 4 customer dissatisfaction
  - 4 employee stress/ dissatisfaction/attrition
  - 2 reputational damage

22

Case studies

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT



Ipsos | Exploring organisational experiences of cyber security breaches

Exploring Organisational Experiences of Cyber Security Breaches

Report

Ipsos

Ipsos

21-094613 | DRAFT VERION 1 | Internal Use Only | This work will be carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with theIpsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Ipsos MORI 2022

- Each one describes:
  - Level of existing cyber security before the breach
  - The breach and the organisation's immediate response
  - Impacts upon the organisation
  - How cyber security arrangements have changed in the wake of a cyber breach
- Let's look at a few examples, by increasing size of business, focusing on what happened as a result of the breach

23

23

Breaches and lessons learned

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

Case Study 5

Micro (<10 employees)

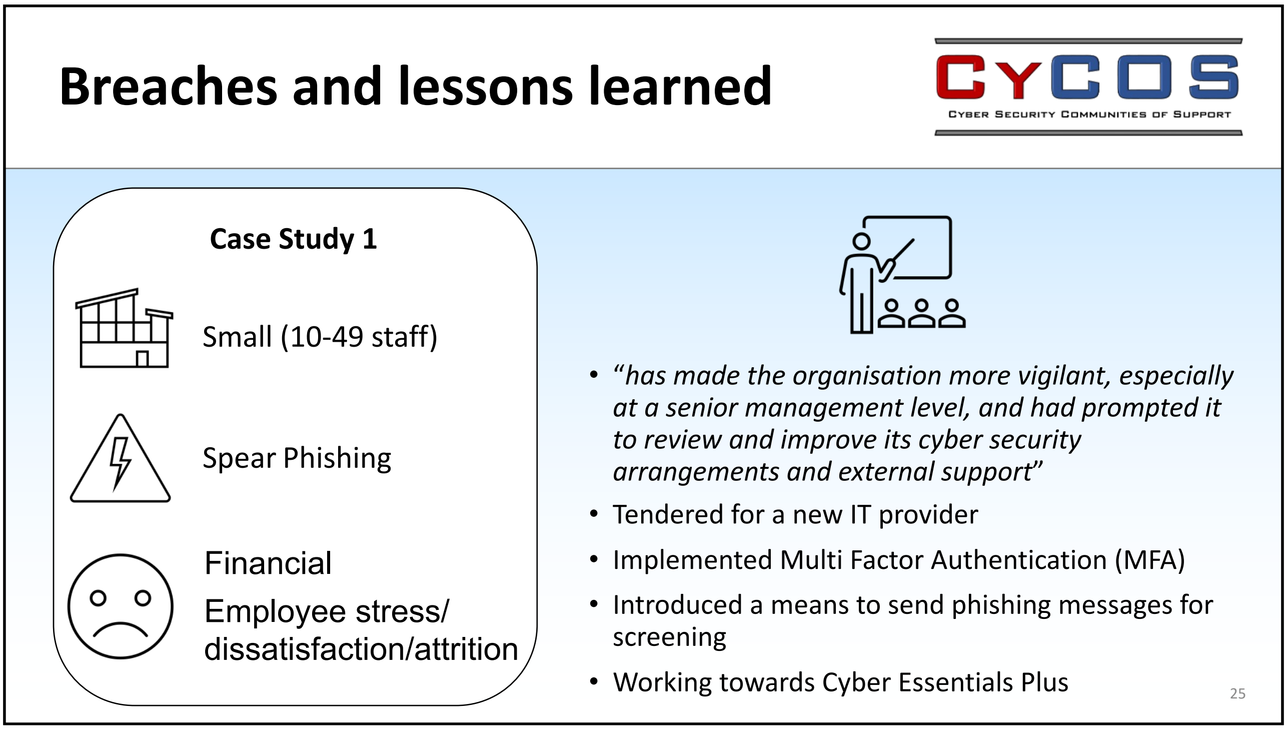
Denial of Service

Financial
Customer dissatisfaction
Reputational damage

- Purchased a new firewall (£400) which 'as soon as it gets bombarded will block out IP addresses'
- MD imposed 'an unofficial policy' that all employees should go to them before opening any 'strange looking emails'
- Taken no further action as they do not have funds for further investment in cyber security training, hardware, or software

24

24



Breaches and lessons learned

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

Case Study 1

Small (10-49 staff)

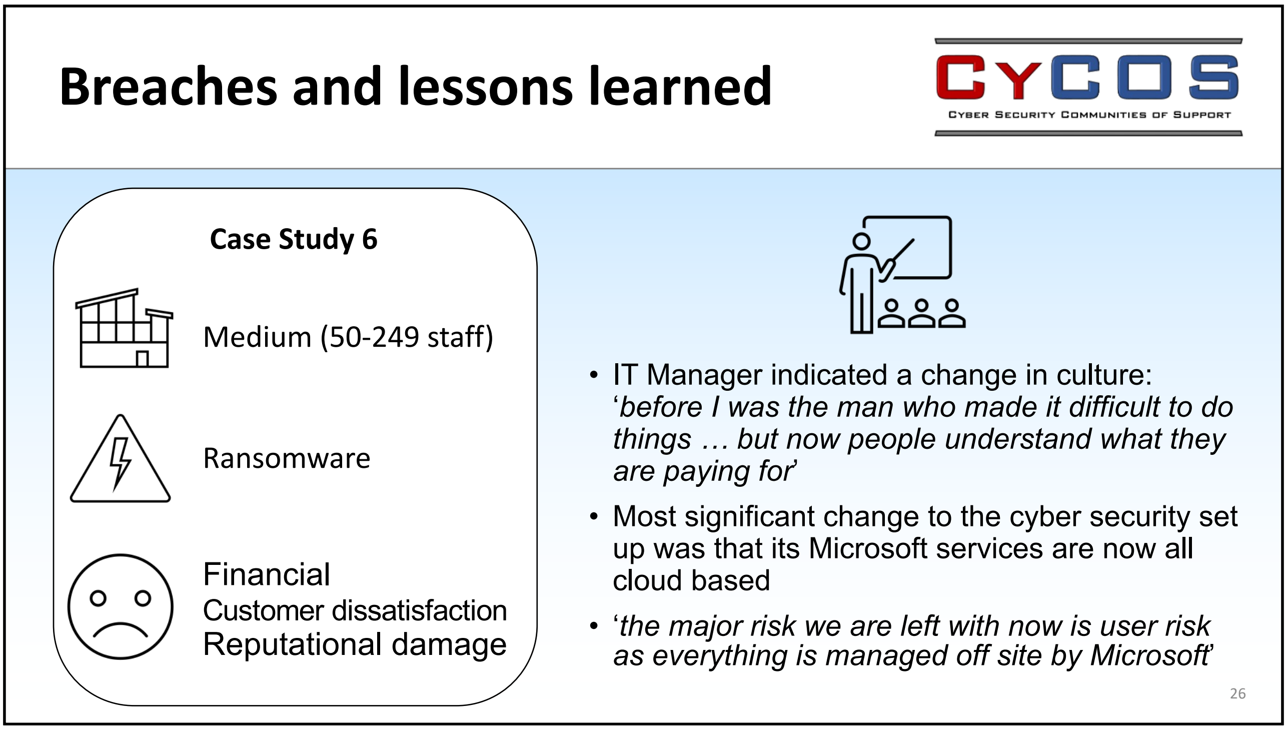
Spear Phishing

Financial
Employee stress/
dissatisfaction/attrition

- *"has made the organisation more vigilant, especially at a senior management level, and had prompted it to review and improve its cyber security arrangements and external support"*
- Tendered for a new IT provider
- Implemented Multi Factor Authentication (MFA)
- Introduced a means to send phishing messages for screening
- Working towards Cyber Essentials Plus

25

25



Breaches and lessons learned

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

Case Study 6

Medium (50-249 staff)

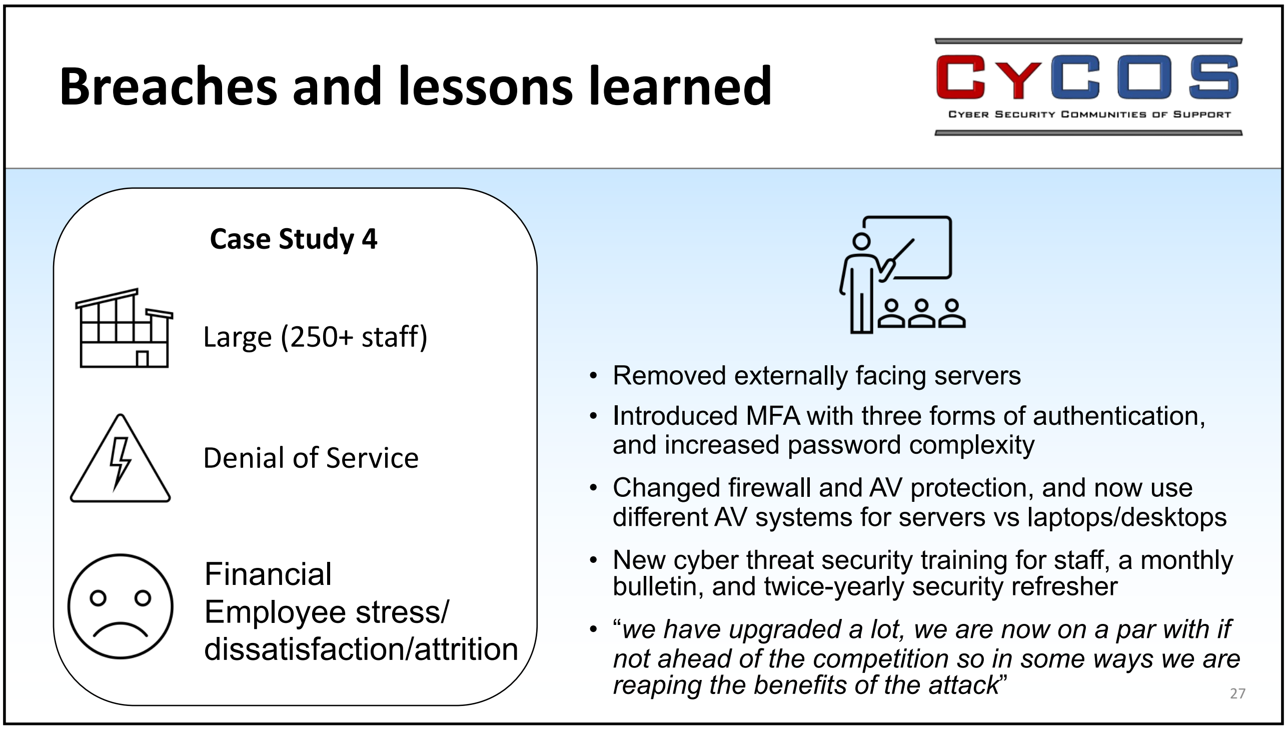
Ransomware

Financial
Customer dissatisfaction
Reputational damage

- IT Manager indicated a change in culture: '*before I was the man who made it difficult to do things … but now people understand what they are paying for*'
- Most significant change to the cyber security set up was that its Microsoft services are now all cloud based
- '*the major risk we are left with now is user risk as everything is managed off site by Microsoft*'

26

26



Breaches and lessons learned

Case Study 4

Large (250+ staff)

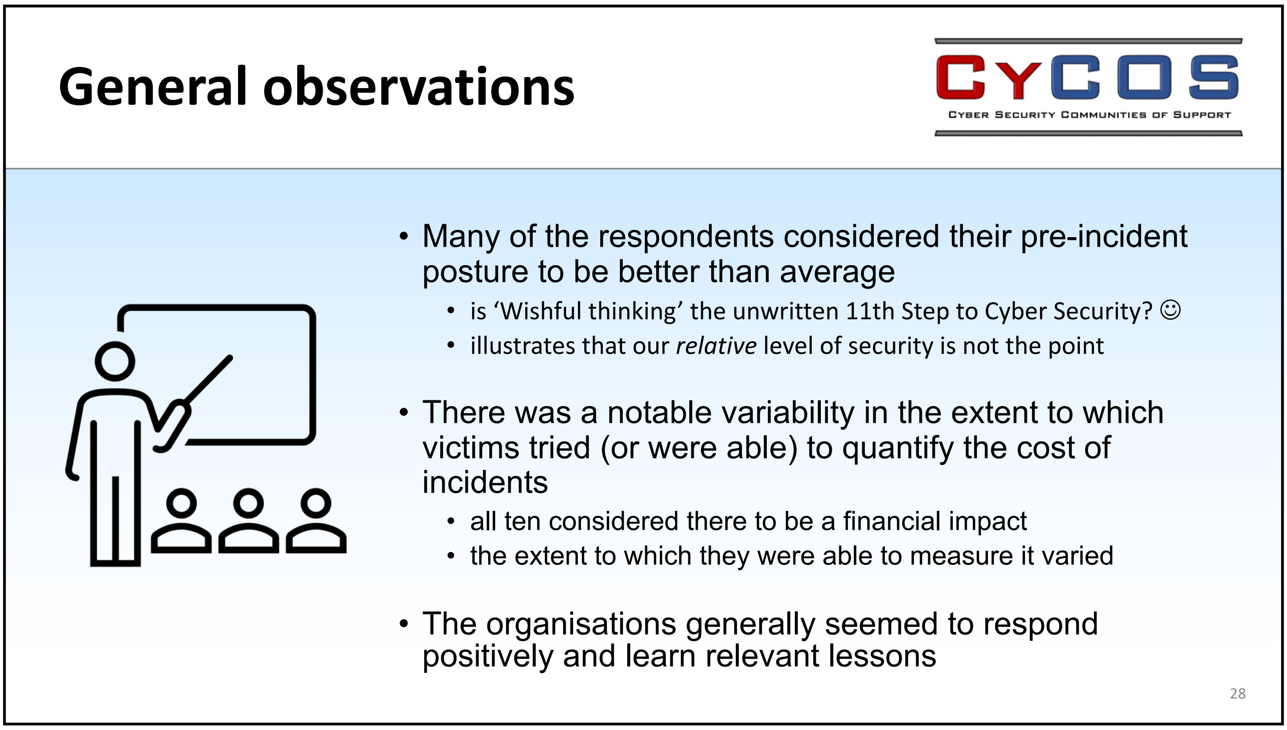
Denial of Service

Financial
Employee stress/
dissatisfaction/attrition

- Removed externally facing servers
- Introduced MFA with three forms of authentication, and increased password complexity
- Changed firewall and AV protection, and now use different AV systems for servers vs laptops/desktops
- New cyber threat security training for staff, a monthly bulletin, and twice-yearly security refresher
- “*we have upgraded a lot, we are now on a par with if not ahead of the competition so in some ways we are reaping the benefits of the attack*”

27

27

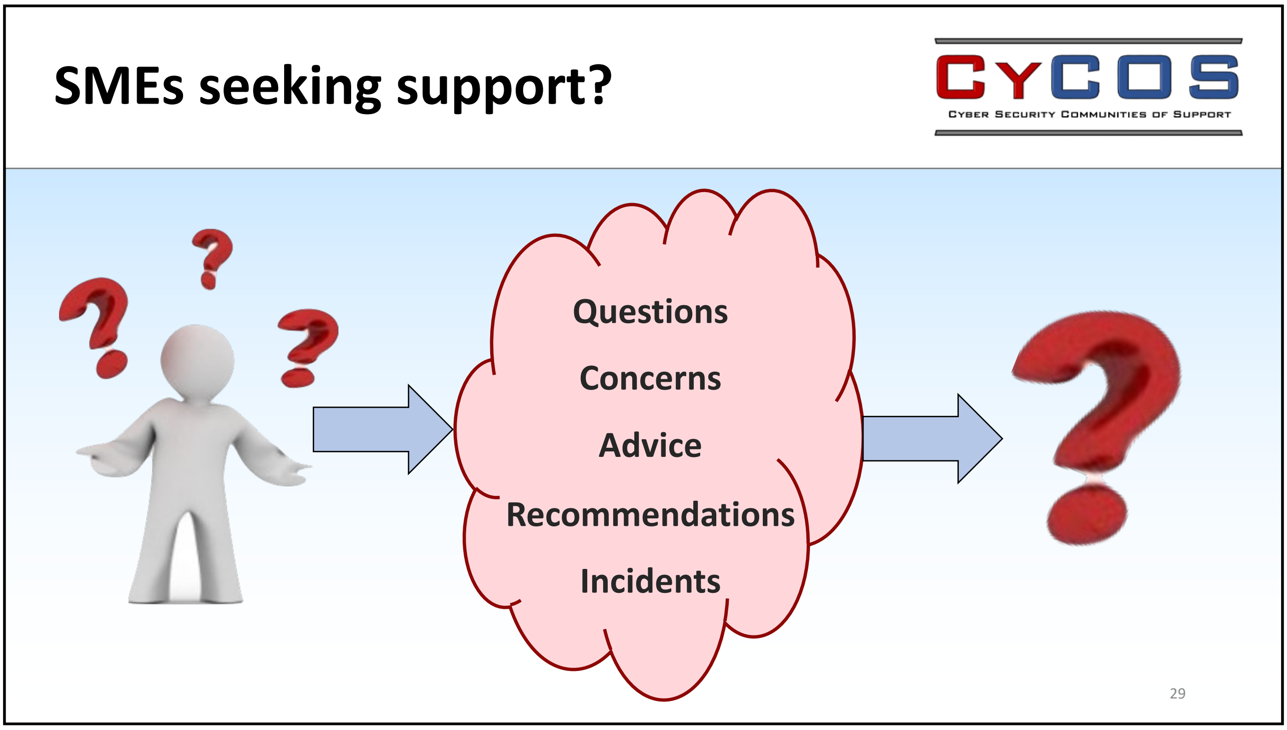


General observations

- Many of the respondents considered their pre-incident posture to be better than average
  - is ‘Wishful thinking’ the unwritten 11th Step to Cyber Security? ☺
  - illustrates that our *relative* level of security is not the point
- There was a notable variability in the extent to which victims tried (or were able) to quantify the cost of incidents
  - all ten considered there to be a financial impact
  - the extent to which they were able to measure it varied
- The organisations generally seemed to respond positively and learn relevant lessons

28

28



SMEs seeking support?

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

Questions

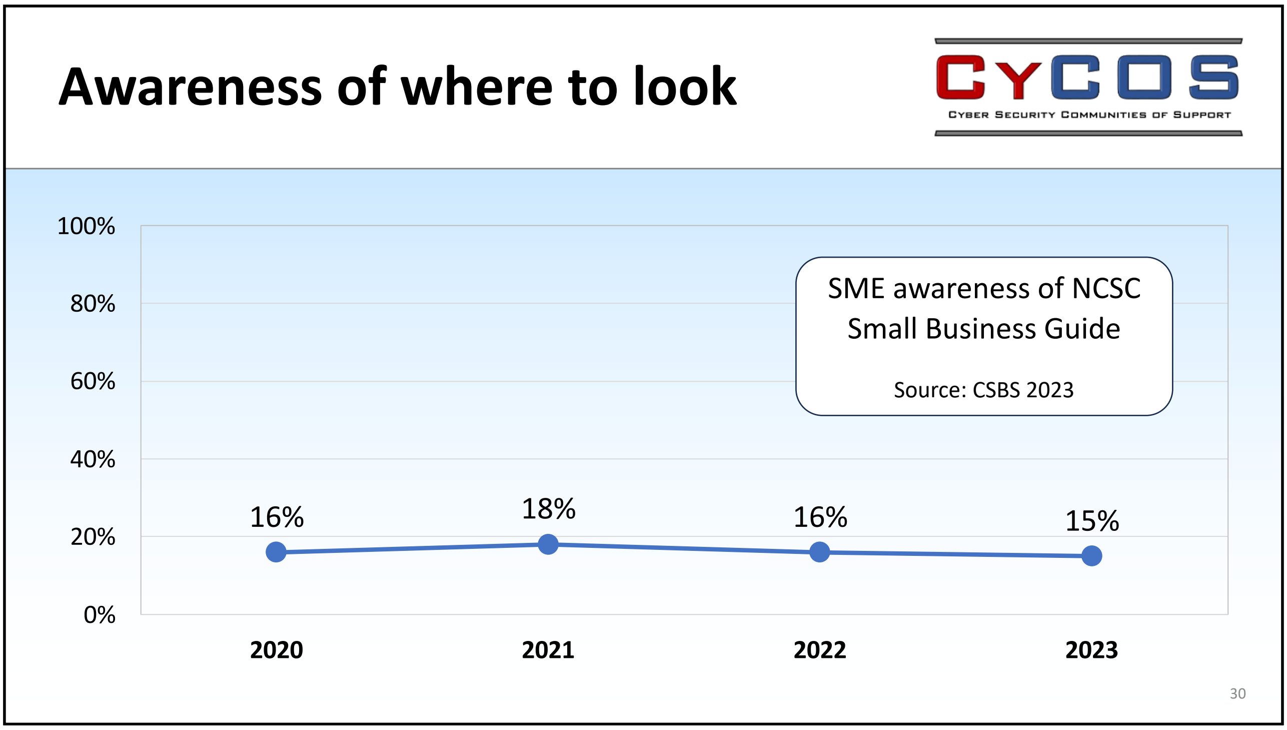
Concerns

Advice

Recommendations

Incidents

29



Awareness of where to look

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

SME awareness of NCSC Small Business Guide

Source: CSBS 2023

30

Guises of guidance
NCSC

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

National Cyber Security Centre

Cyber Security
Small Business Guide

Small Business Guide Collection

How to improve your cyber security; affordable, practical advice for businesses

- Step 1 - Backing up your data
- Step 2 - Protecting your organisation from malware
- Step 3 - Keeping your smartphones (and tablets) safe
- Step 4 - Using passwords to protect your data
- Step 5 - Avoiding phishing attacks

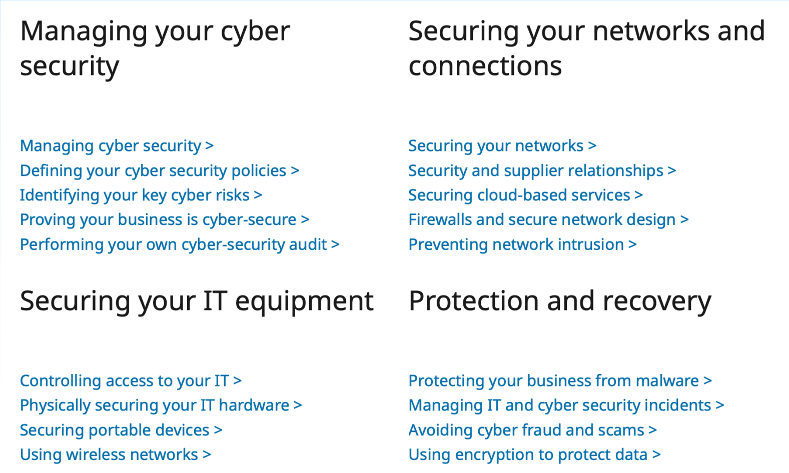
www.ncsc.gov.uk/collection/small-business-guide

31

31

Guises of guidance
bsi website

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT



Managing your cyber security

Managing cyber security >
Defining your cyber security policies >
Identifying your key cyber risks >
Proving your business is cyber-secure >
Performing your own cyber-security audit >

Securing your networks and connections

Securing your networks >
Security and supplier relationships >
Securing cloud-based services >
Firewalls and secure network design >
Preventing network intrusion >

Securing your IT equipment

Controlling access to your IT >
Physically securing your IT hardware >
Securing portable devices >
Using wireless networks >

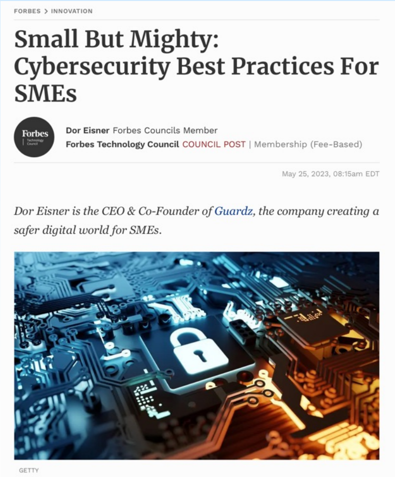
Protection and recovery

Protecting your business from malware >
Managing IT and cyber security incidents >
Avoiding cyber fraud and scams >
Using encryption to protect data >

www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/

32

Guises of guidance
Forbes website



FORBES > INNOVATION

Small But Mighty: Cybersecurity Best Practices For SMEs

Dor Eisner Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

May 25, 2023, 08:15am EDT

Dor Eisner is the CEO & Co-Founder of Guardz, the company creating a safer digital world for SMEs.

GETTY

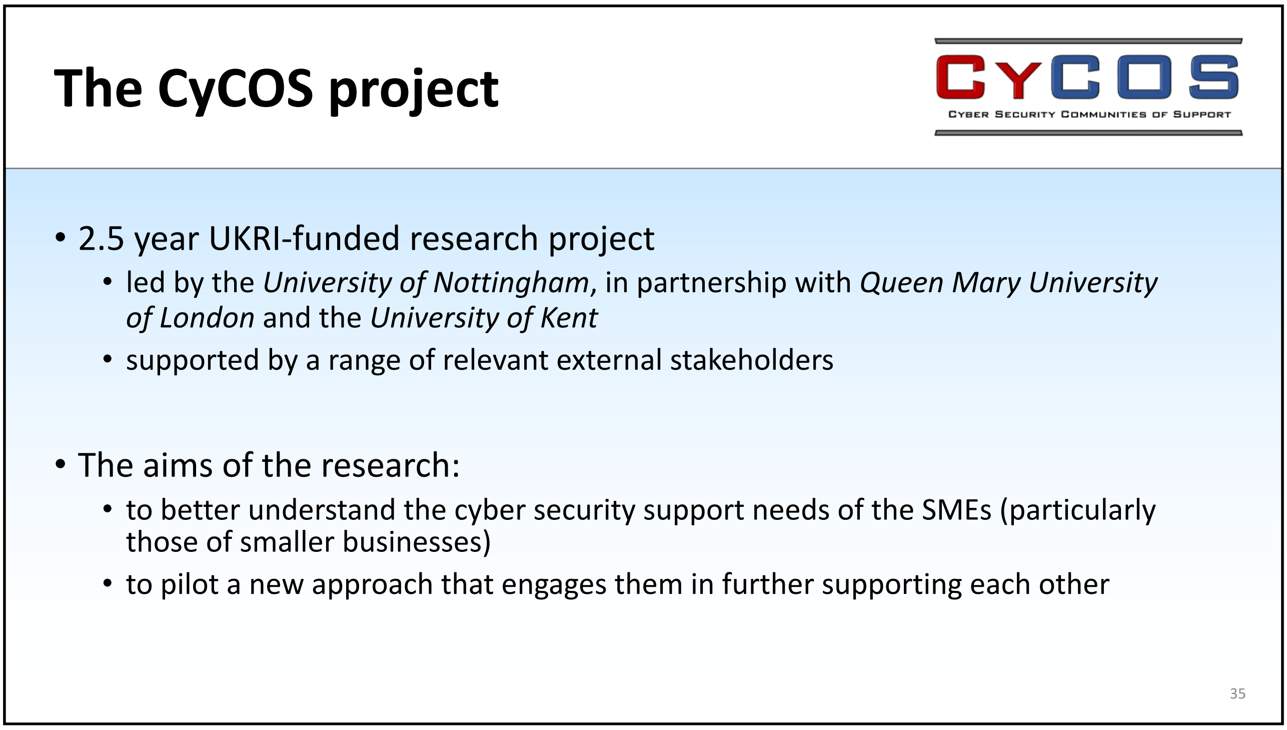
- Conduct Real-Time Cyber Awareness Training
- Leverage The Latest Tech: AI Is Happening
- Acquire Cyber Insurance
- Safeguard Digital Assets Everywhere
- Mind Your Business

www.forbes.com/sites/forbestechcouncil/2023/05/25/small-but-mighty-cybersecurity-best-practices-for-smes/

Journey’s end?

How do they feel?

and has security been improved?



The CyCOS project

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

- 2.5 year UKRI-funded research project
  - led by the *University of Nottingham*, in partnership with *Queen Mary University of London* and the *University of Kent*
  - supported by a range of relevant external stakeholders
- The aims of the research:
  - to better understand the cyber security support needs of the SMEs (particularly those of smaller businesses)
  - to pilot a new approach that engages them in further supporting each other

35

35

Academic investigators

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

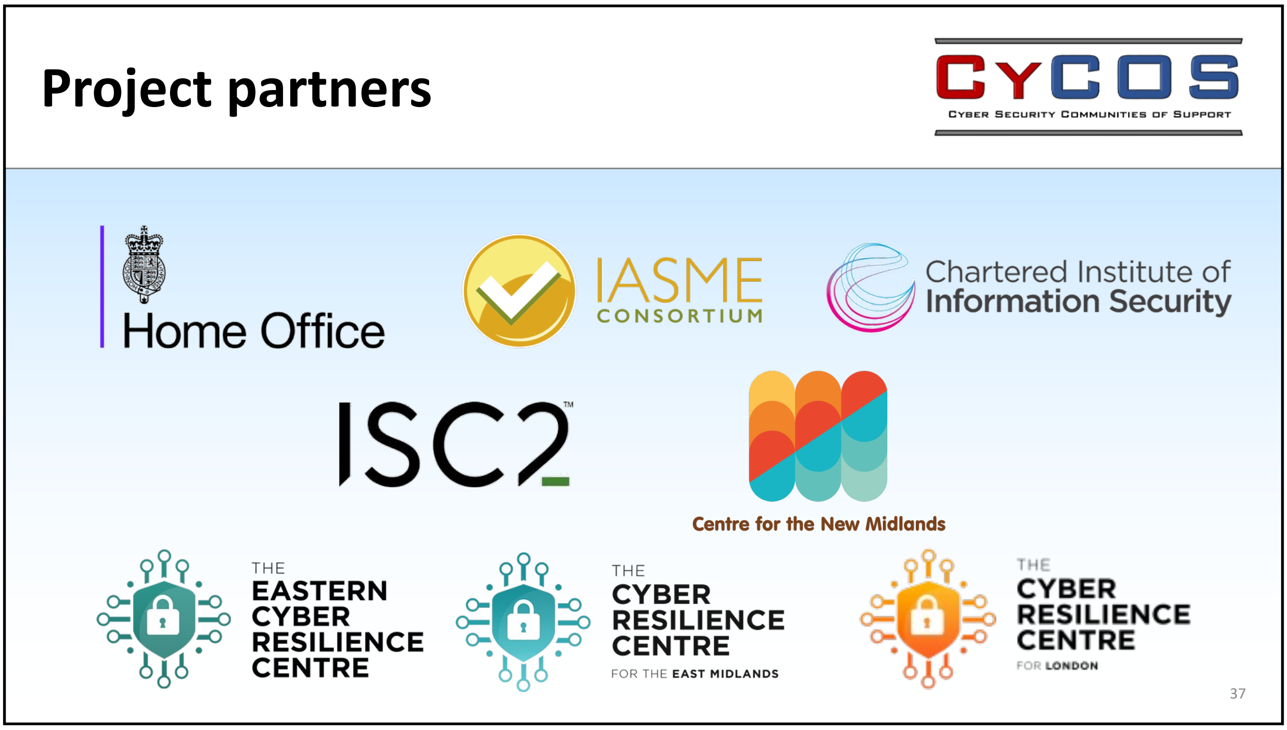
Prof. Steven Furnell
University of Nottingham

Dr Maria Bada
Queen Mary University of London

Dr Jason Nurse
University of Kent

36

36



Project partners

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

Home Office

IASME CONSORTIUM

Chartered Institute of Information Security

ISC2™

Centre for the New Midlands

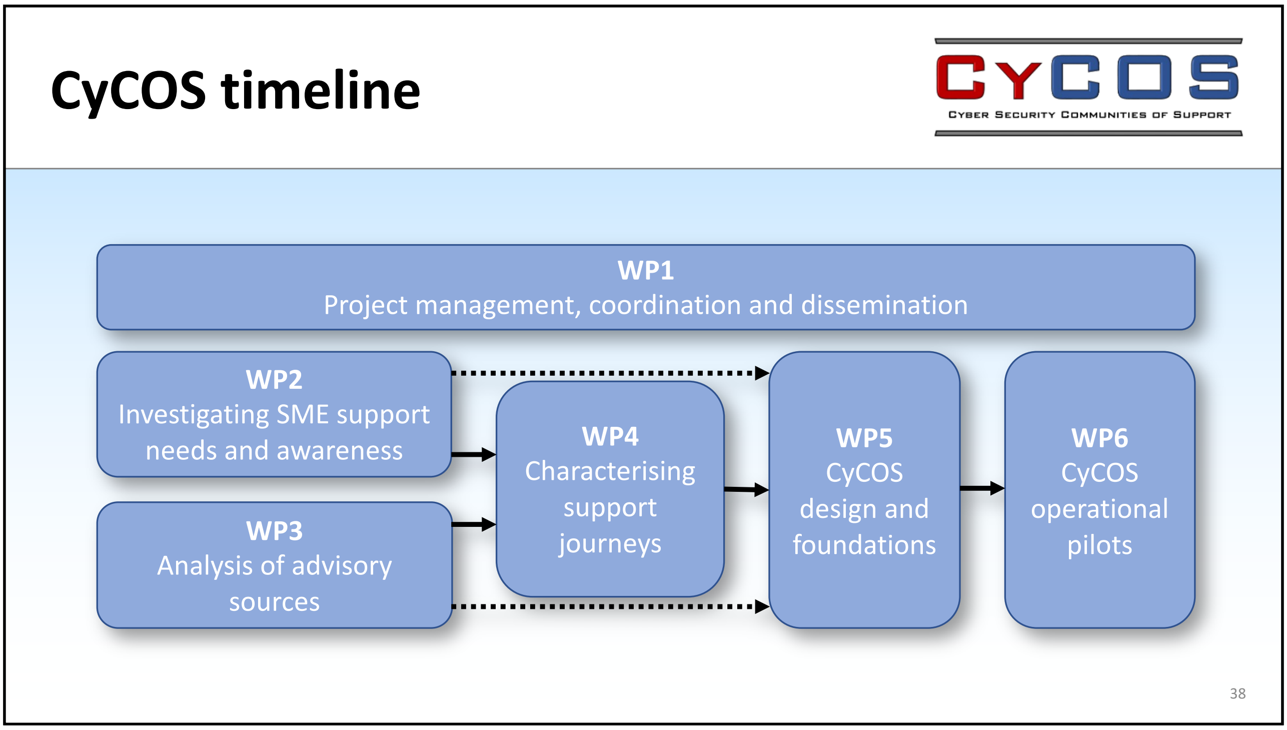
THE EASTERN CYBER RESILIENCE CENTRE

THE CYBER RESILIENCE CENTRE FOR THE EAST MIDLANDS

THE CYBER RESILIENCE CENTRE FOR LONDON

37

37



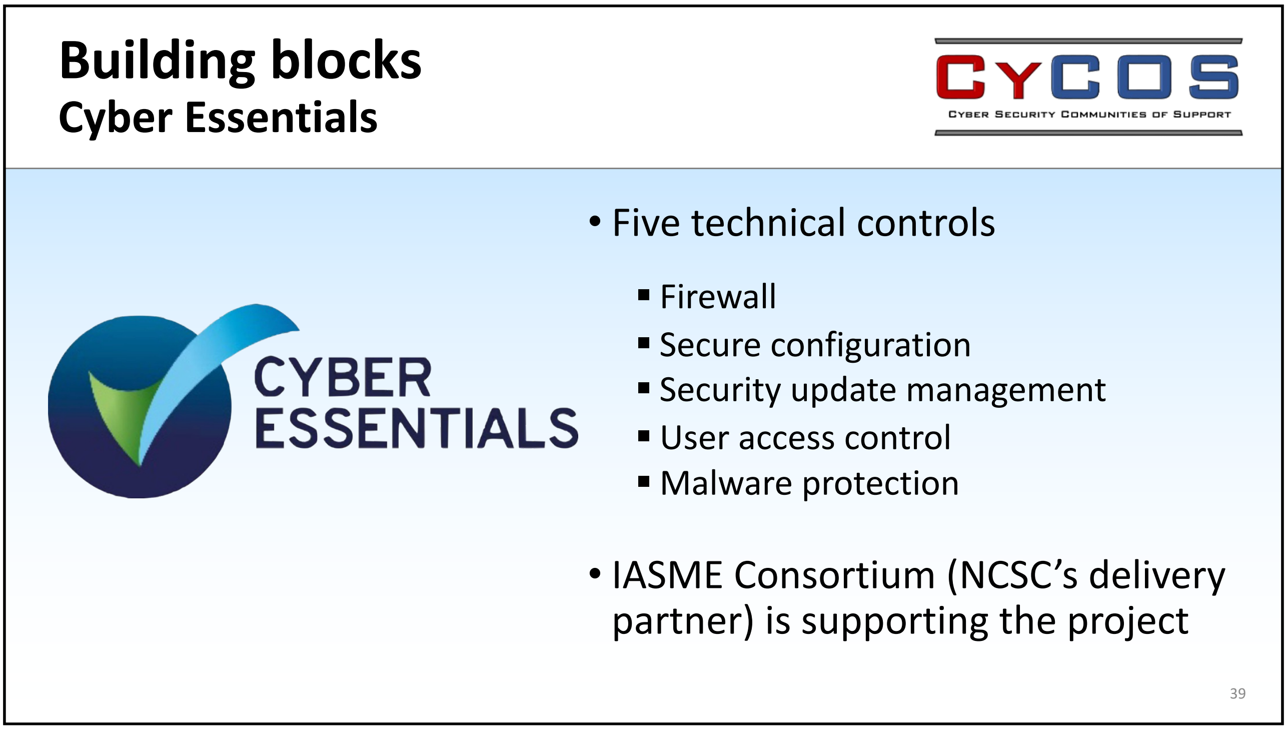
CyCOS timeline

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

WP1
Project management, coordination and dissemination
WP2
Investigating SME support needs and awareness
WP3
Analysis of advisory sources
WP4
Characterising support journeys
WP5
CyCOS design and foundations
WP6
CyCOS operational pilots

38

38



Building blocks
Cyber Essentials

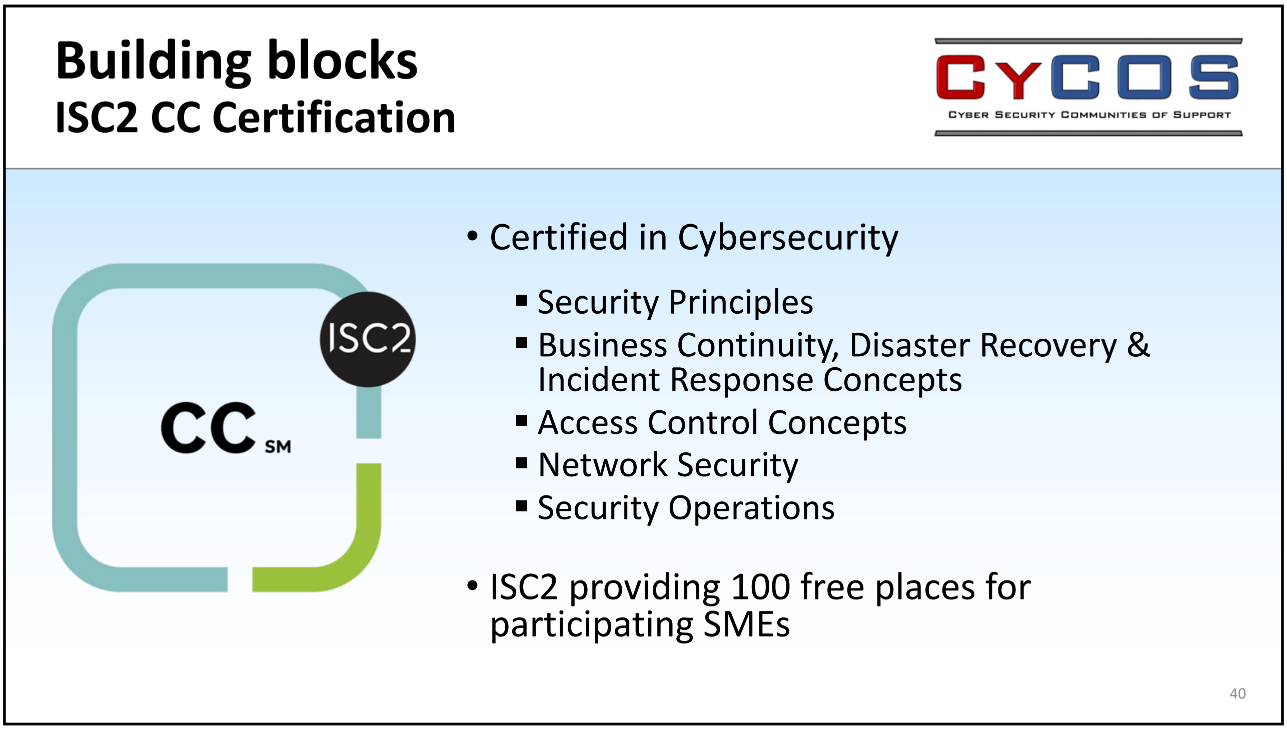
CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

CYBER ESSENTIALS

- Five technical controls
  - Firewall
  - Secure configuration
  - Security update management
  - User access control
  - Malware protection
- IASME Consortium (NCSC’s delivery partner) is supporting the project

39

39



Building blocks
ISC2 CC Certification

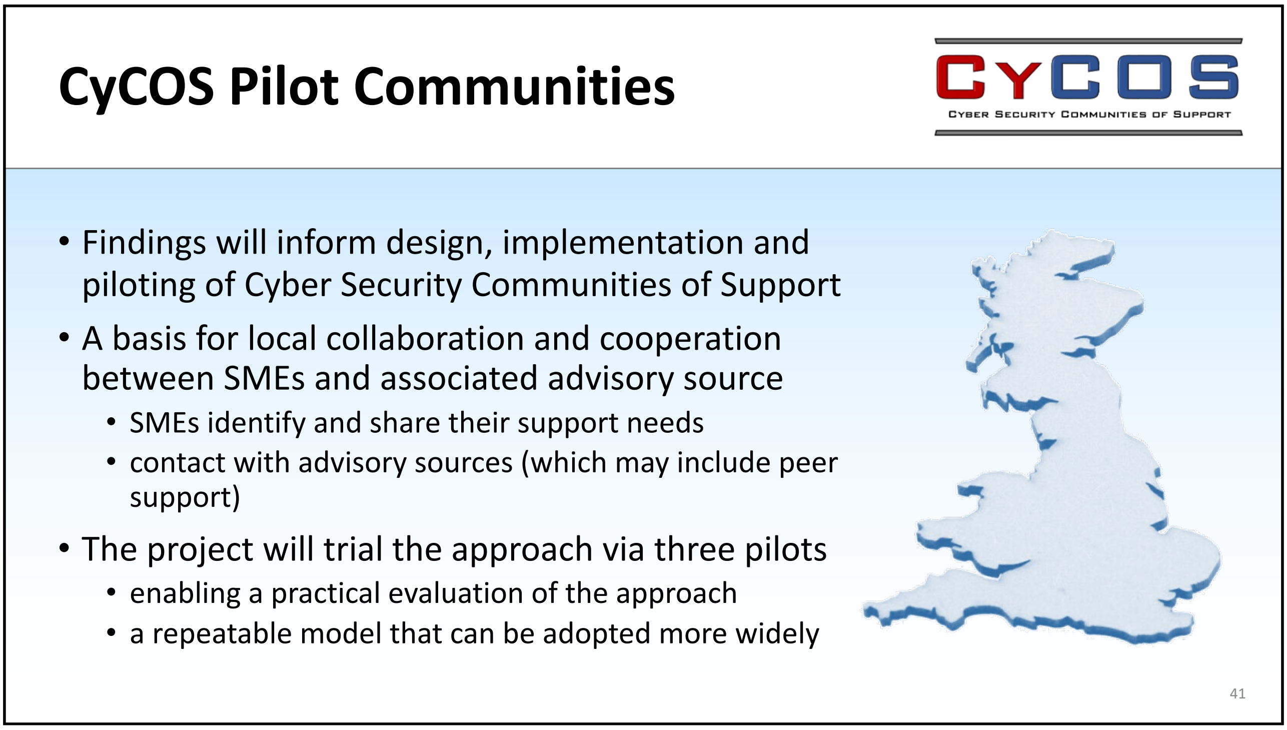
CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

ISC2 CC SM

- Certified in Cybersecurity
  - Security Principles
  - Business Continuity, Disaster Recovery & Incident Response Concepts
  - Access Control Concepts
  - Network Security
  - Security Operations
- ISC2 providing 100 free places for participating SMEs

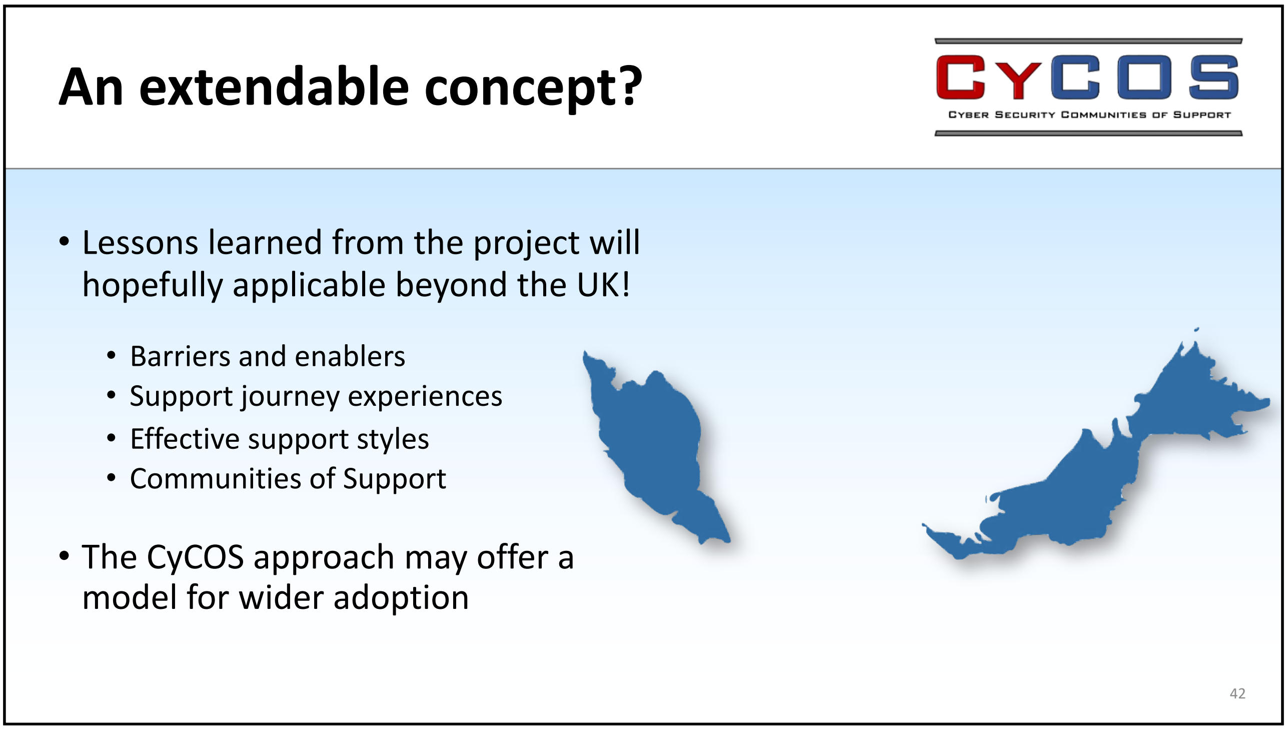
40

40



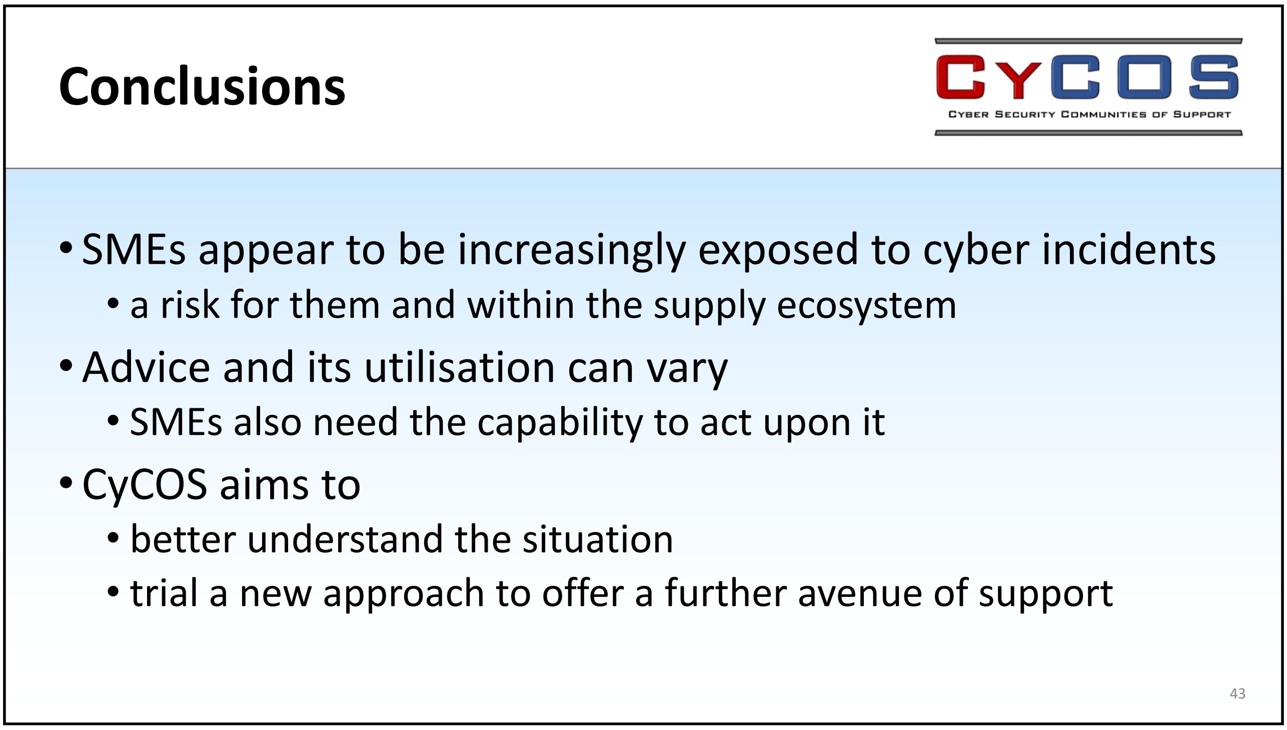
CyCOS Pilot Communities

- Findings will inform design, implementation and piloting of Cyber Security Communities of Support
- A basis for local collaboration and cooperation between SMEs and associated advisory source
  - SMEs identify and share their support needs
  - contact with advisory sources (which may include peer support)
- The project will trial the approach via three pilots
  - enabling a practical evaluation of the approach
  - a repeatable model that can be adopted more widely



An extendable concept?

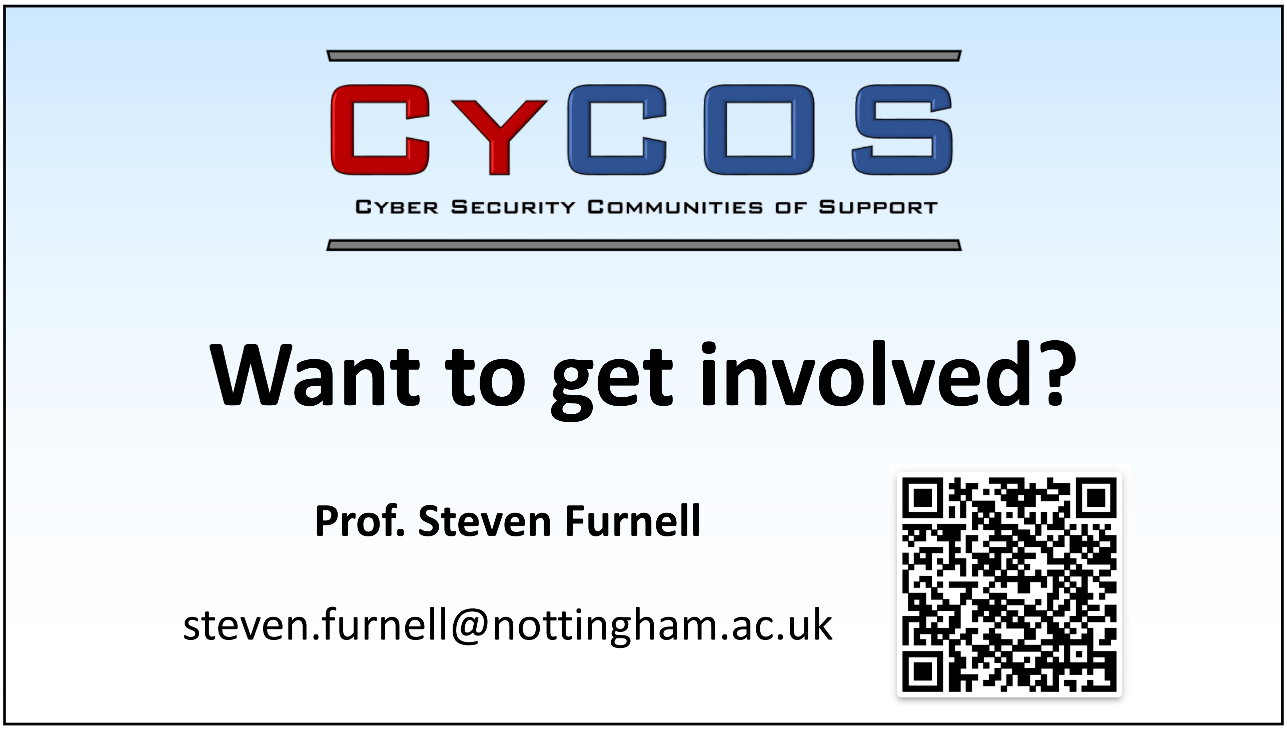
- Lessons learned from the project will hopefully applicable beyond the UK!
  - Barriers and enablers
  - Support journey experiences
  - Effective support styles
  - Communities of Support
- The CyCOS approach may offer a model for wider adoption



Conclusions

CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

- SMEs appear to be increasingly exposed to cyber incidents
  - a risk for them and within the supply ecosystem
- Advice and its utilisation can vary
  - SMEs also need the capability to act upon it
- CyCOS aims to
  - better understand the situation
  - trial a new approach to offer a further avenue of support



CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT

Want to get involved?

Prof. Steven Furnell

steven.furnell@nottingham.ac.uk