
University of
Nottingham
UK | CHINA | MALAYSIA
Cyber Security – Why me, I'm an SME?
Professor Steven Furnell , Professor of Cyber Security, School of Computer Science
5th December 2023

1


CYCOS
CYBER SECURITY COMMUNITIES OF SUPPORT
Cyber Security
Why me, I'm an SME?
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

2

Outline

- Introduction
- Cyber Security incidents in SMEs
- Key guidance
- The CyCOS project
- Current support
  - Cyber Essentials (Peter Loomes)
  - The East Midlands Cyber Resilience Centre (Colin Ellis)
- Q&A

3

3

Introduction

- Cybersecurity is an ongoing challenge for *all* organisations
  - technology usage and network connectivity are fundamental for modern businesses
- 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 larger organisations

4

4

SMEs and cyber security

- Small businesses may lack 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*

5

5

A lack of skills?

- 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 at a disadvantage
  - potentially exposed
  - dependent upon further support in the event of incidents, or when making security-related decisions

6

6

My main source …


Department for Science, Innovation & Technology

Official Statistics

Cyber security breaches survey 2023

Published 19 April 2023

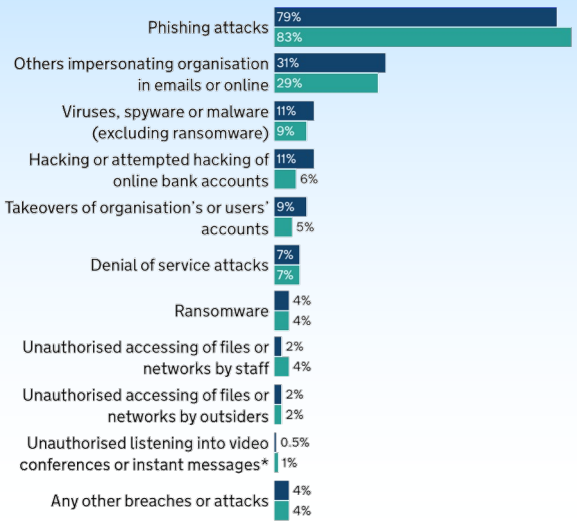
Contents

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

7

7

Breaches and attacks



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

8

8

Dangerous decline?

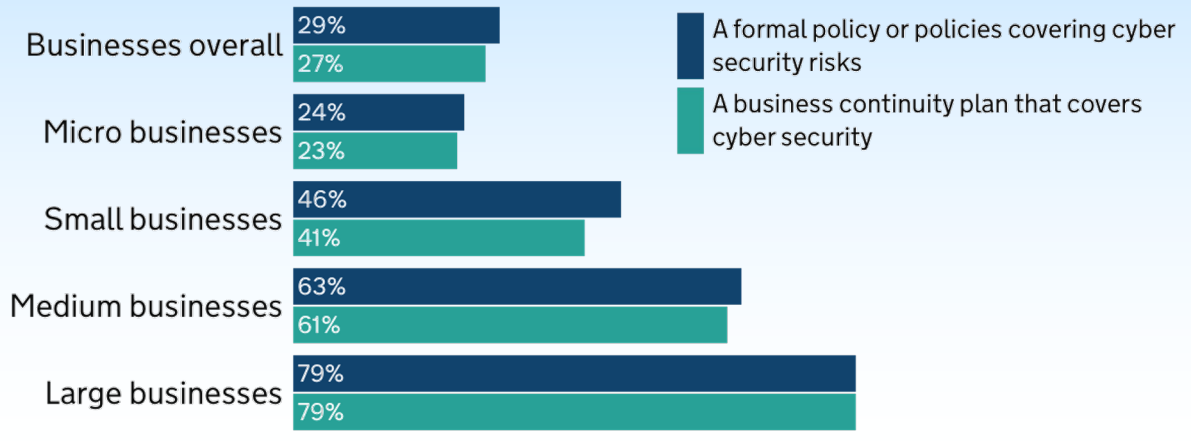
- The proportion of micro businesses saying cyber security is a high priority has decreased from 80% in 2022 to 68%
- Basic cyber hygiene practices have fallen:
  - use of password policies (79% in 2021, vs. 70% in 2023)
  - use of network firewalls (78% in 2021 vs. 66% in 2023)
  - restricting admin 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

9

9

Who does what?



10

10

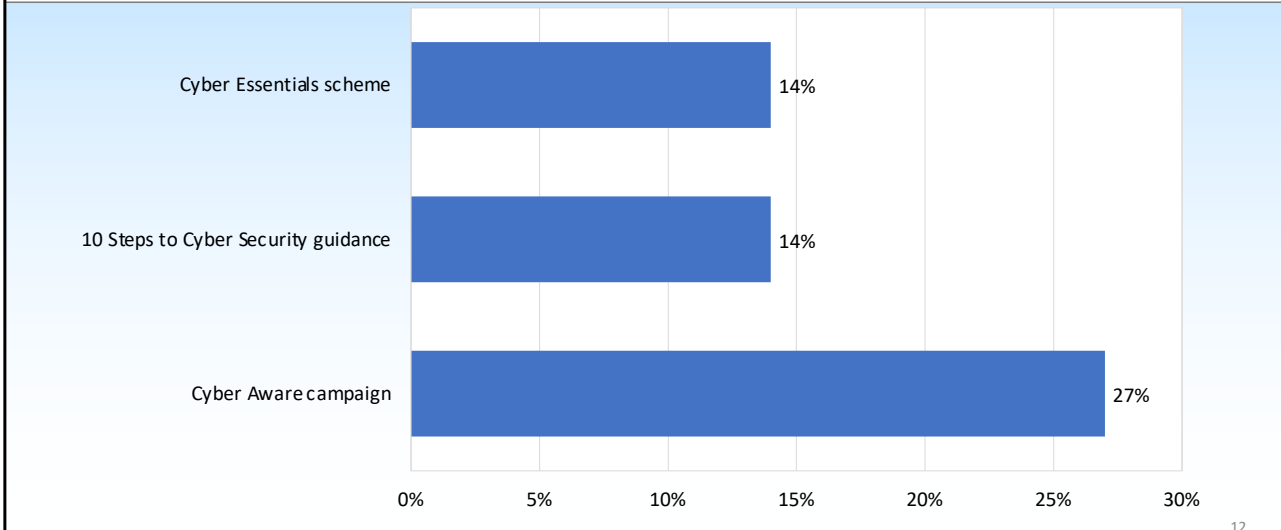
Things SMEs could be aware of

- **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

11

11

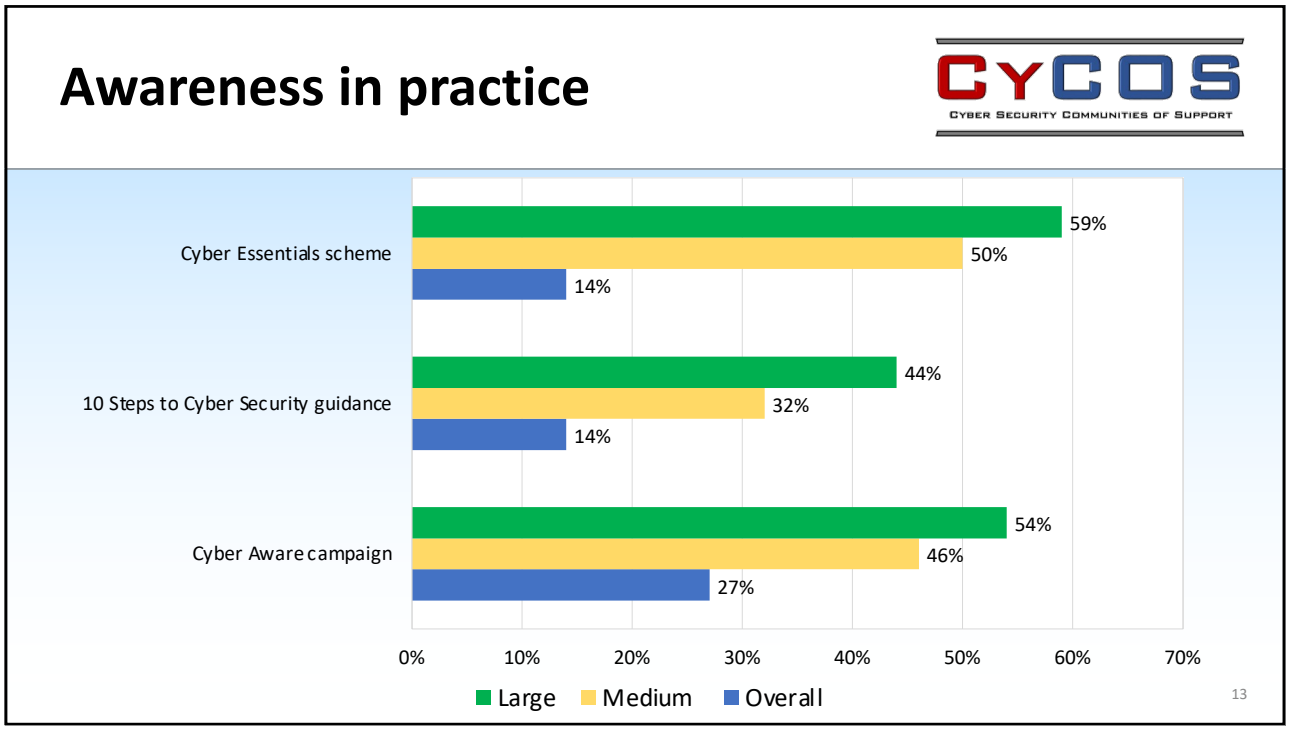
Awareness in practice



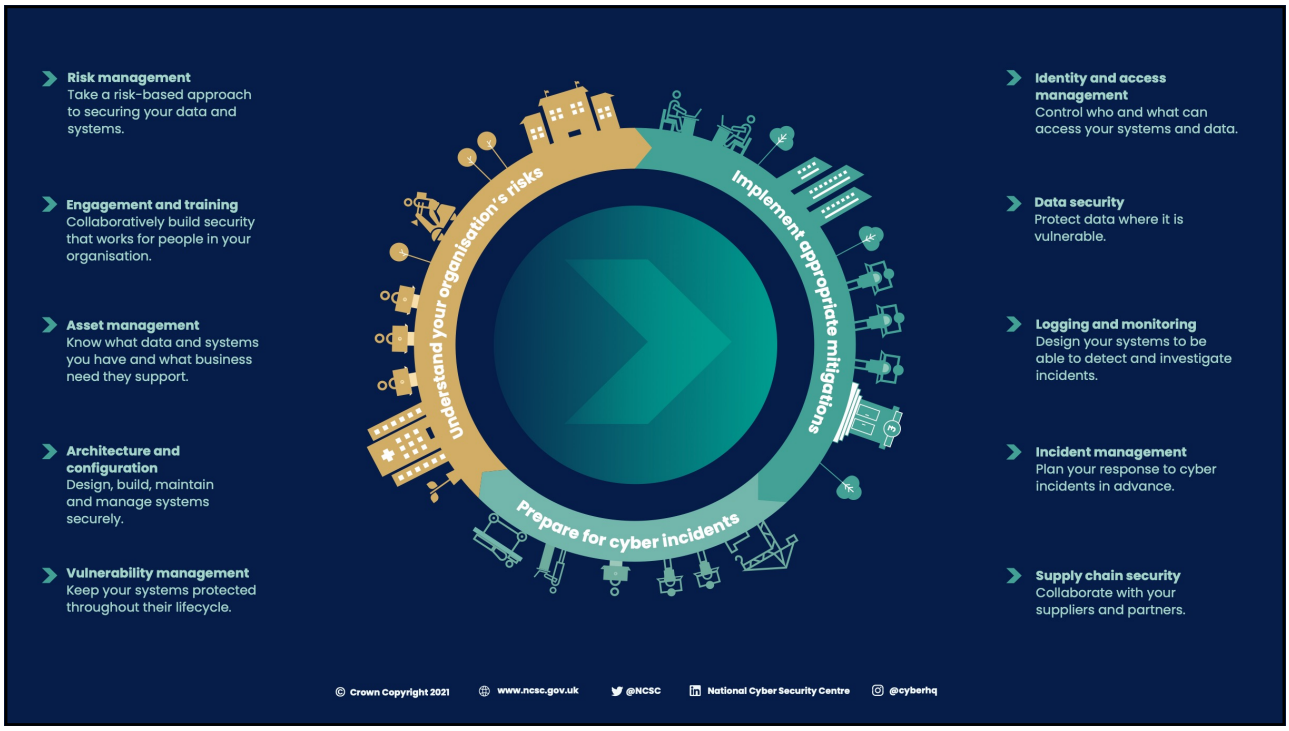
12

12

Awareness in practice

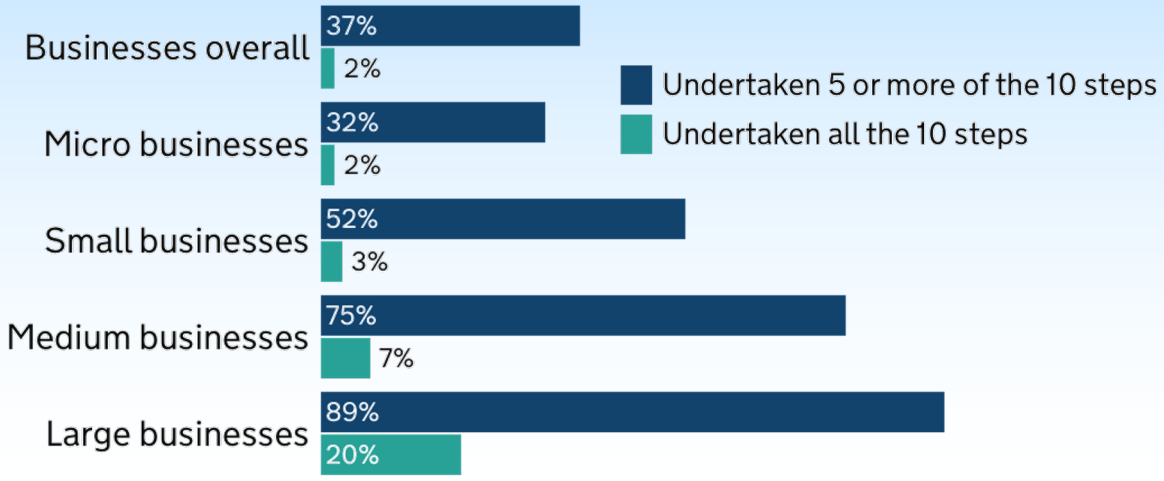


13



14

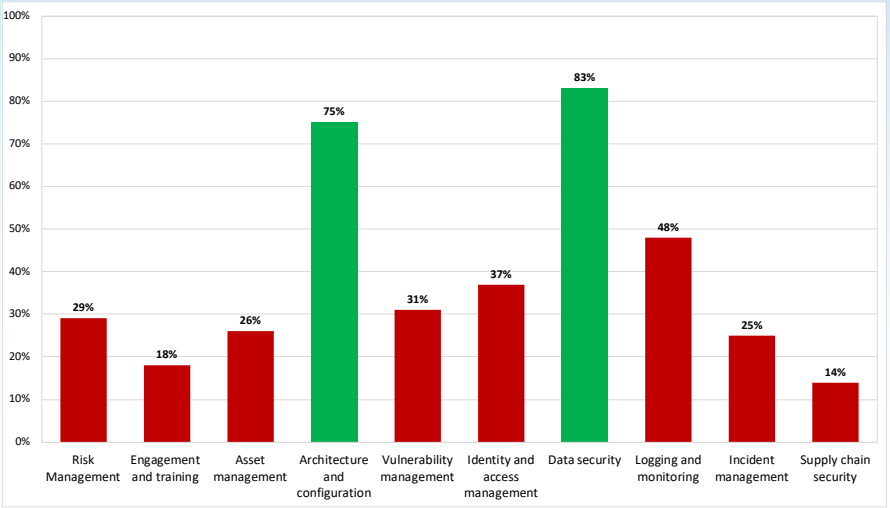
Who does what?



15

15

Taking the Steps in practice …

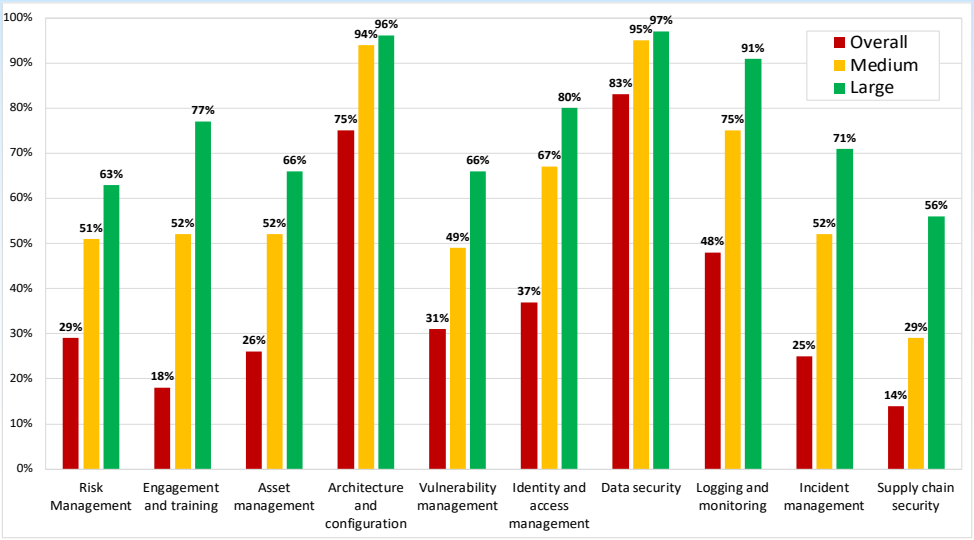


Source: *Cyber Security Breaches Survey 2023*

16

16

Taking the Steps in practice …

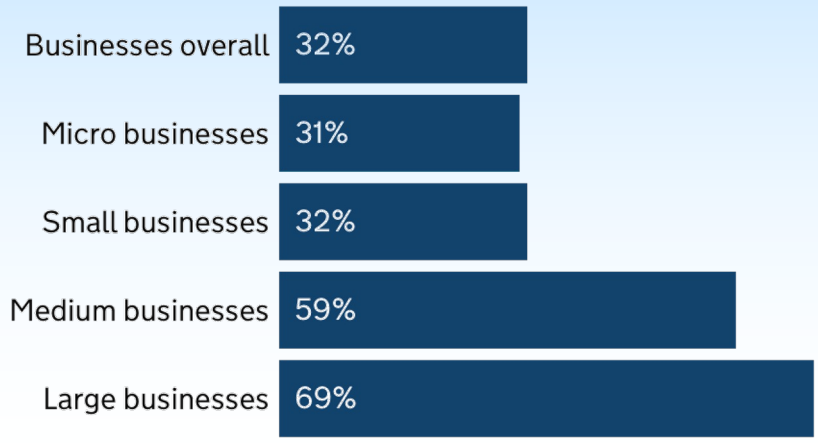


Source: *Cyber Security Breaches Survey 2023*

17

17

Does it matter?

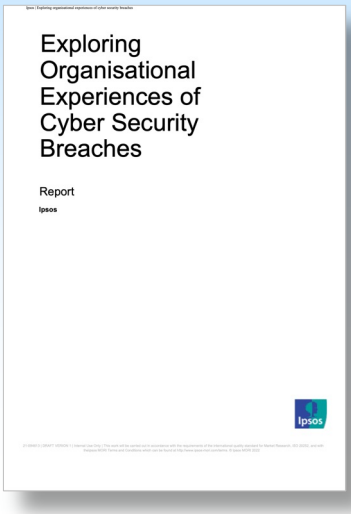


Percentage of organisations that have identified breaches or attacks in the last 12 months

18

18

Case examples



- **Organisations:**
  - 1 micro
  - 2 small
  - 3 medium
  - 4 large
- **Breaches:**
  - 3 Denial-of-Service
  - 3 Ransomware
  - 3 Spear Phishing
  - 1 Smishing

www.gov.uk/government/publications/exploring-organisational-experiences-of-cyber-security-breaches

19

19

Guidance to follow

- **NCSC Small Business Guide**
  - Five key steps, each with five related tips
  - Links to further related material

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

20

20

Step 1 - Backing up your data

- Tip 1: Identify what data you need to back up
- Tip 2: Keep your backup separate from your computer
- Tip 3: Consider the cloud
- Tip 4: Read our cloud security guidance
- Tip 5: Make backing up part of your everyday business

21

21

Step 2 - Protecting your organisation from malware

- Tip 1: Install (and turn on) antivirus software
- Tip 2: Prevent staff from downloading dodgy apps
- Tip 3: Keep all your IT equipment up to date (patching)
- Tip 4: Control how USB drives (and memory cards) can be used
- Tip 5: Switch on your firewall

22

22

Step 3 - Keeping your smartphones (and tablets) safe

- Tip 1: Switch on password protection
- Tip 2: Make sure lost or stolen devices can be tracked, locked or wiped
- Tip 3: Keep your device up to date
- Tip 4: Keep your apps up to date
- Tip 5: Don't connect to unknown Wi-Fi Hotspots

23

23

Step 4 - Using passwords to protect your data

- Tip 1: Make sure you switch on password protection
- Tip 2: Use 2-step verification for 'important' accounts
- Tip 3: Avoid using predictable passwords
- Tip 4: Help your staff cope with 'password overload'
- Tip 5: Change all default passwords

24

24

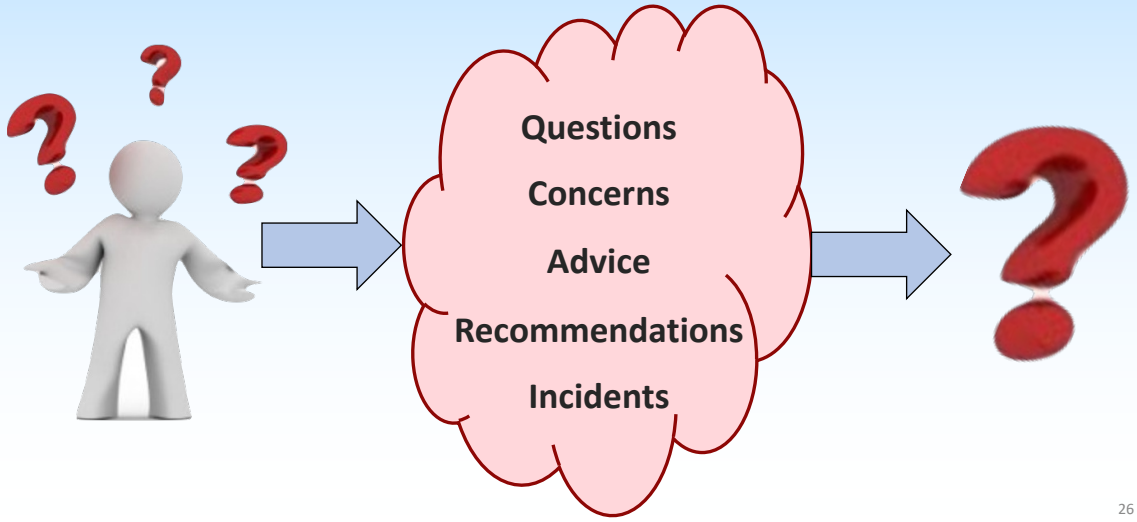
Step 5 - Avoiding phishing attacks

- Tip 1: Configure accounts to reduce the impact of successful attacks
- Tip 2: Think about how you operate
- Tip 3: Check for the obvious signs of phishing
- Tip 4: Report all attacks
- Tip 5: Check your digital footprint

25

25

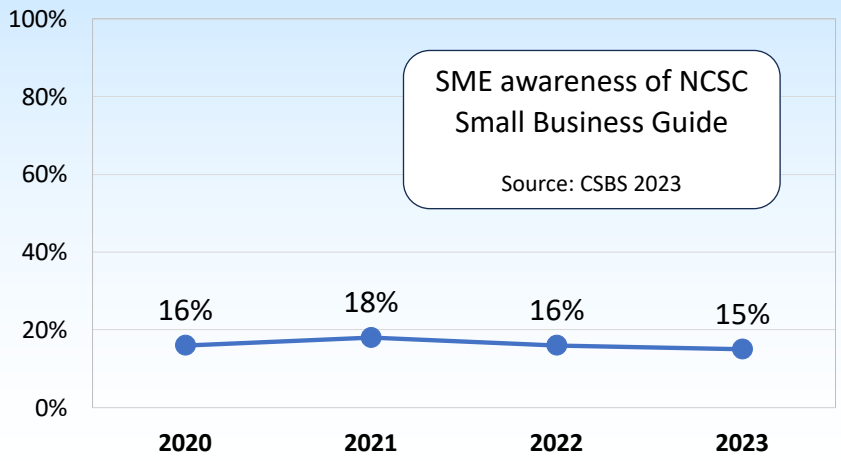
Seeking support?



26

26

Awareness of where to look



27

27

Guises of guidance
bsi website

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/

28

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/

29

29

Journey's end?

How do you feel?

and has security been improved?

30

30

The CyCOS project

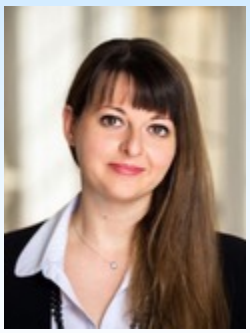
- 2.5 year UKRI-funded research project
  - led by the *University of Nottingham*, in partnership with *Queen Mary University of London* and the *University of Kent*
  - supported by a range of relevant external stakeholders
- The aims of the research:
  - to better understand the cyber security support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

31

31

Project team

Prof. Steven Furnell
University of Nottingham



Dr Maria Bada
Queen Mary University of London

Dr Jason Nurse
University of Kent

Dr Neeshé Khan
University of Nottingham

32

32

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

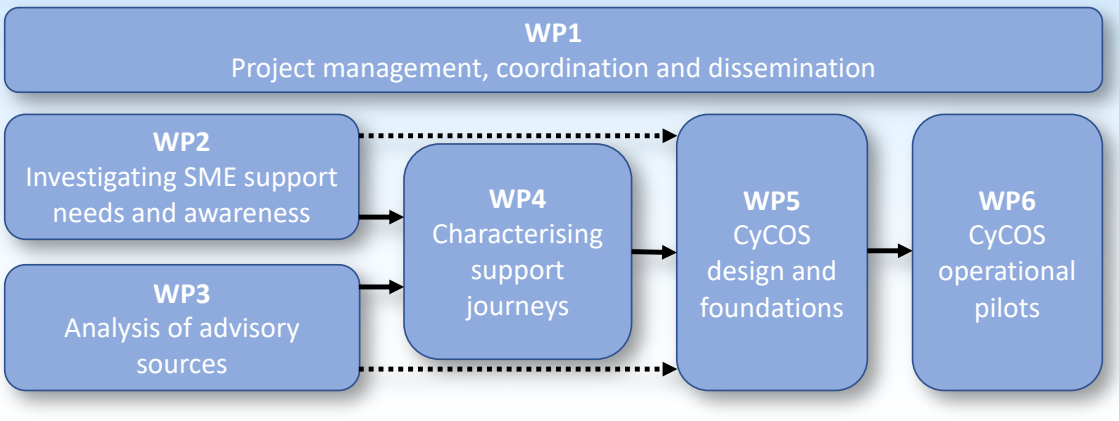
THE CYBER RESILIENCE CENTRE FOR LONDON

33

33

CyCOS timeline

CyCOS Cyber Security Communities of Support



34

34

Building blocks
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

35

35

Building blocks
ISC2 CC Certification

- 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

36

36

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

37

37

Conclusions

- 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

38

38

We want you ☺

We would welcome ~10 minutes of your time to share your understanding and experience of cyber security, and your existing use of available advice and support

https://app.onlinesurveys.jisc.ac.uk/s/qmul/cycos

39

39