Cybersecurity Awareness and Capacities of SMEs

Gencer Erdogan, Ragnhild Halvorsrud, Costas Boletsis,
Simeon Tverdal, John Brian Pickering

9th International Conference on Information Systems Security and Privacy (ICISSP'23)

Lisbon, Portugal, 22-24 February 2023

Technology for a better society

Outline

- Survey intro and method
- Cybersecurity awareness of SMEs
- Cybersecurity practices of SMEs
- Conclusion

Survey intro and method

Target group

- Employees from SMEs.
- SME: an enterprise fewer than 250 persons (EC).
- In total, 141 SMEs based in the UK were recruited.
- One participant per SME.

Sampling and data collection

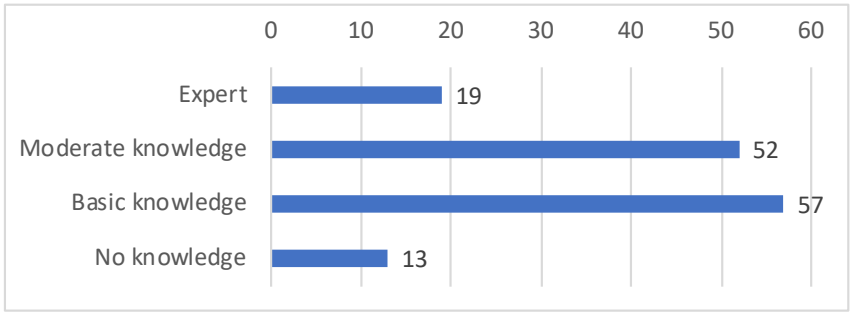
- UK was chosen because 40% of UK-based businesses report on security breaches and attacks.
- Approach respondents in their native language.
- Recruitment via Norstat recruitment agency for online research. QuenchTec.

Questionnaire design

- Iteratively developed and piloted with N=23 participants.
- In total 27 questions: company, participant, infrastructure, cybersecurity awareness, cybersecurity practices.
- Focus of this paper: awareness and practices. 13 questions.

Knowledge of the employees and their company's awareness

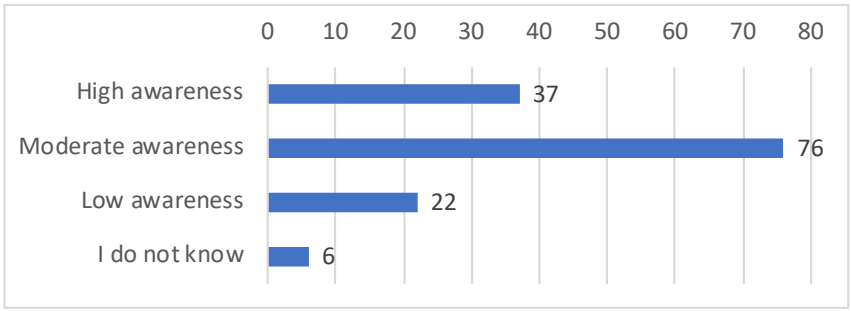
How would you characterize your own knowledge about cybersecurity?



- 19+52=71 of the 141 respondents (50%) characterize their own cybersecurity-knowledge as moderate or expert.

- only 51 of the 141 respondents work with cybersecurity, but 71 assess themselves as moderate/expert:
The perception about their own security awareness is rather optimistic.

How would you characterize your company when it comes to cybersecurity awareness?

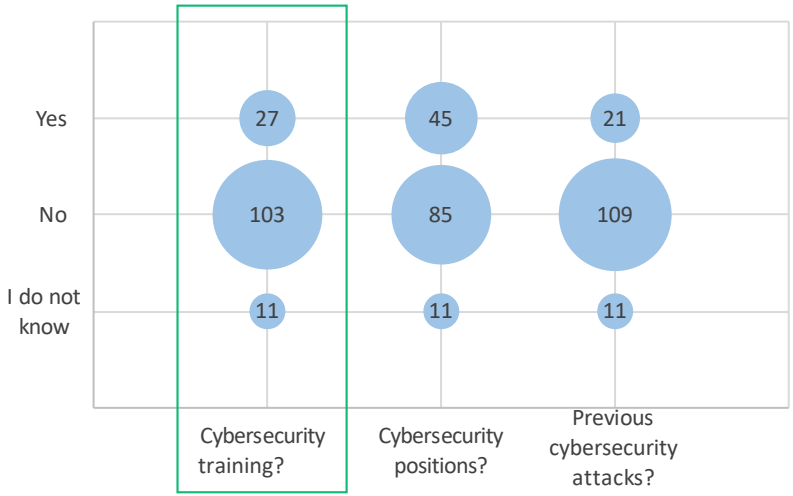


- 37+76=113 of the 141 respondents (80%) characterize their company's cybersecurity-awareness as moderate or high.

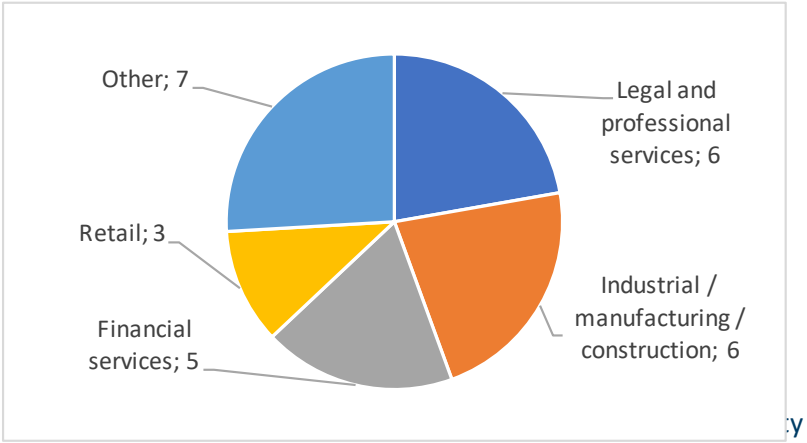
- People tend to trust that cybersecurity is dealt with in other parts of the company. "If people think someone else is responsible, then they won't take action themselves" (Paek & Hove, 2017).

Training capabilities

Does your company offer courses or training material for employees to raise awareness about cybersecurity?

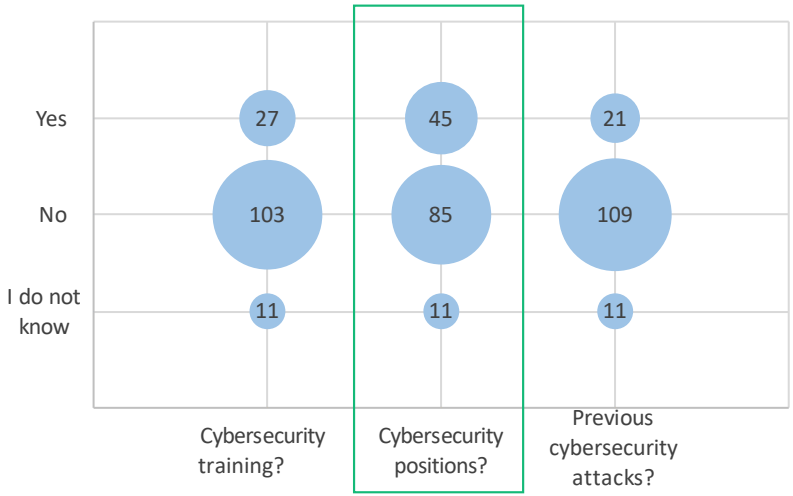


- Despite the 50% moderate to high cybersecurity awareness, only 27 provide cybersecurity training for their employees.
- The training offered is limited to the basics of security and privacy that employees need to be aware of at work.
- The frequency of training is either once at onboarding or at best yearly repetitions.
- Domains:



Security positions

Does your company have positions dedicated to cybersecurity at any level?



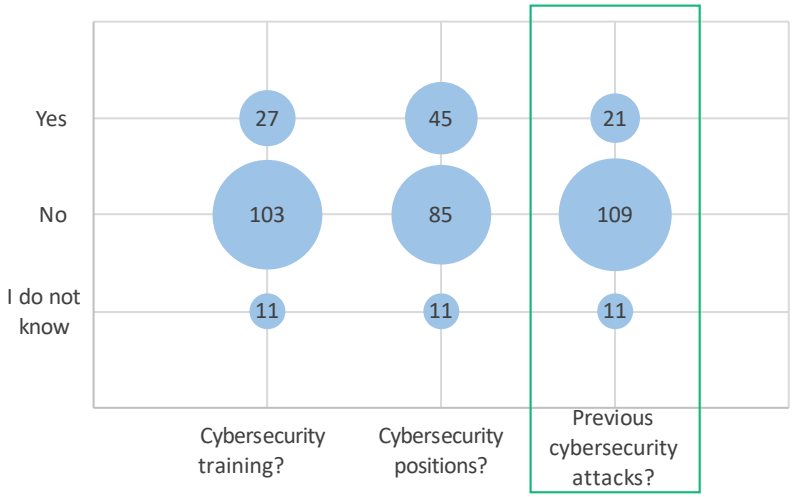
- 45 of the 141 respondents (32%) confirm that their SME have positions dedicated to cybersecurity.

- The question regarding dedicated cybersecurity positions scored the highest (45 out of 141) compared to other yes/no questions. This indicates that the SMEs should be better prepared than indicated in the survey results in general.

- Positive: from the 45 respondents that do have cybersecurity positions, the industry sector is quite diverse: Software and computer service, retail, health, manufacturing, financial services, …

Previous cybersecurity attacks

Were there any previous cybersecurity attacks on your company that you know about?

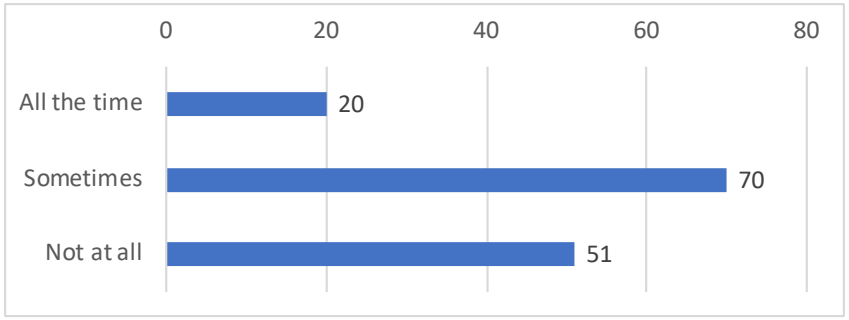


- Only 21 of the 141 respondents (15%) were aware of previous cybersecurity attacks.

- An attack harmed one or more security qualities:
  - 12 attacks altered the integrity of information
  - 11 attacks rendered the information system unavailable
  - 6 attacks caused a breach of confidential information

Discussing cybersecurity issues, and fear of attack

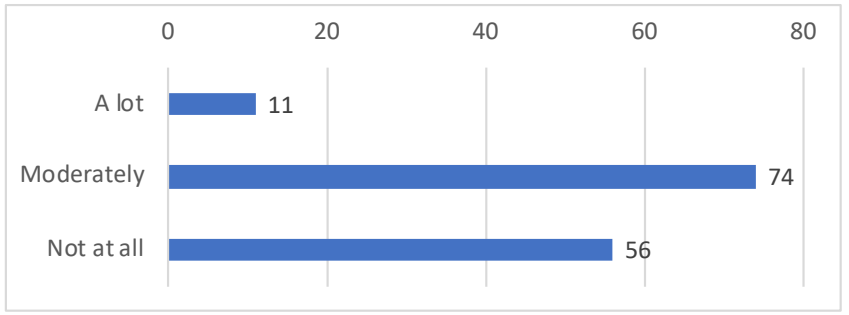
Do you discuss cybersecurity issues on your company meetings or presentations or, in general, internally in your company?



● Only 20 of the 141 respondents (15%) mention that they regularly discuss security issues as part of company processes.

● This indicates a lack of focus on security issues and clear security processes, but this problem is also linked to lack of security positions and available resources.

To what degree do you fear for a cybersecurity attack towards your company?

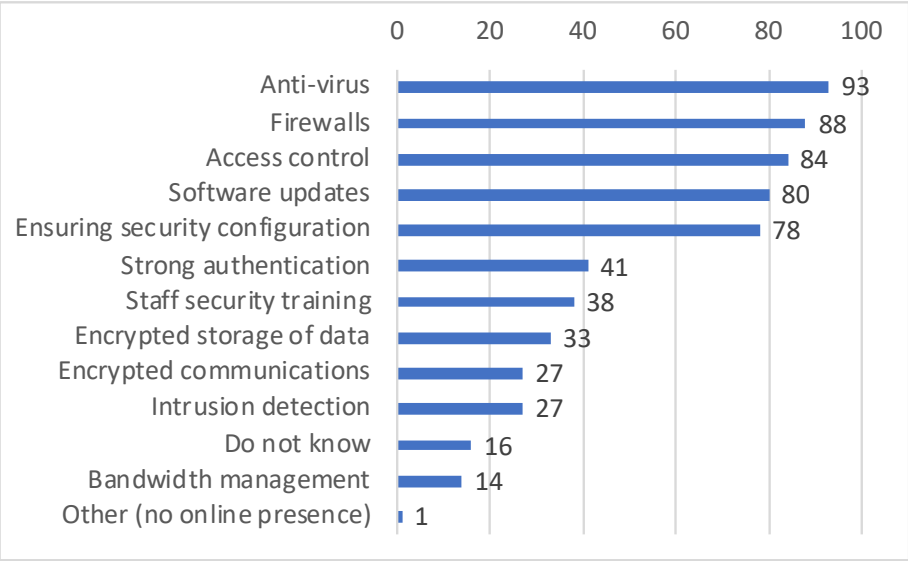


● 11+74=85 of the 141 respondents (60%) have a “moderate” or “a lot” of fear that their company will be attacked.

● SME’s are to some extent aware, but the lack of focus on security, training, dedicated positions, and awareness of attacks may indicate that SME’s do not feel responsible.

Security measures to avoid cybersecurity attacks

What security measures is your company taking to avoid cybersecurity attacks?



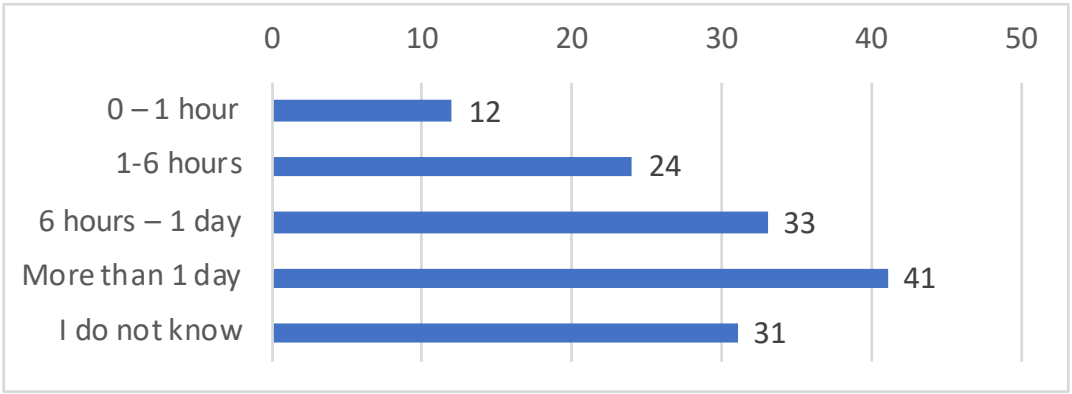
- Basic security tools such as Anti-virus and Firewalls are the main security mechanisms in use.

- Tools for training and the identification of threats and vulnerabilities are less used, but this may be because of lack of appropriate tooling with low threshold.

- SMEs need more training and easy-to-use tools to help carry out tasks such as threat and vulnerability identification and risk assessment.

Availability criticality

How long do you think your critical applications and systems can be shut down before significant disruption is caused to the company?

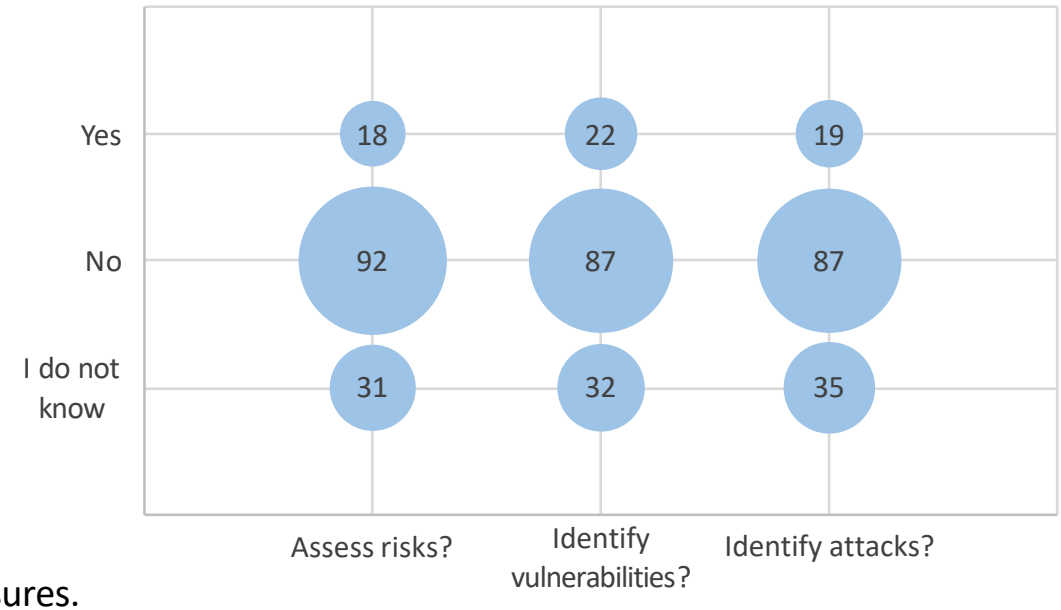


- The fact that 41+31=72 of the 141 respondents (over 50%) replied “more than 1 day” or “I do not know” indicates that the respondents may not have the full overview of their critical assets.

- That is, SME’s need better tool support to assess and understand their critical assets.

Processes and tools

Does your company use specific processes or tools
- to assess risk to its IT assets?
- for identifying vulnerabilities?
- for identifying attacks?



- Hardly any of the SMEs use tools or have processes in place to assess cybersecurity risks, identify vulnerabilities, and identify attacks.

- This indicates lack of appropriate tools to encourage awareness, and tools to easily capture and present threats and their corresponding measures.

Conclusion

- There is an apparent discrepancy between the levels of awareness and knowledge claimed by individuals.
- People tend to trust that security is dealt with in other parts of the company. Lack of individual responsibility taking.
- The training offered is limited to the basics of security and privacy, and there is a lack of appropriate training material and courses.
- Although 45 of the 141 respondents (32%) confirm that their SME have positions dedicated to cybersecurity, there is a lack of supportive low-threshold tools to assess vulnerabilities and cybersecurity risks.
- SMEs need to increase focus on security processes, training, dedicated security positions, and awareness of attacks to better protect themselves from cybersecurity risks.

SINTEF

Technology for a better society