The human factor in cybersecurity

Andreas Andreou (MSc, BA)

Cyprus Neuroscience & Technology Institute

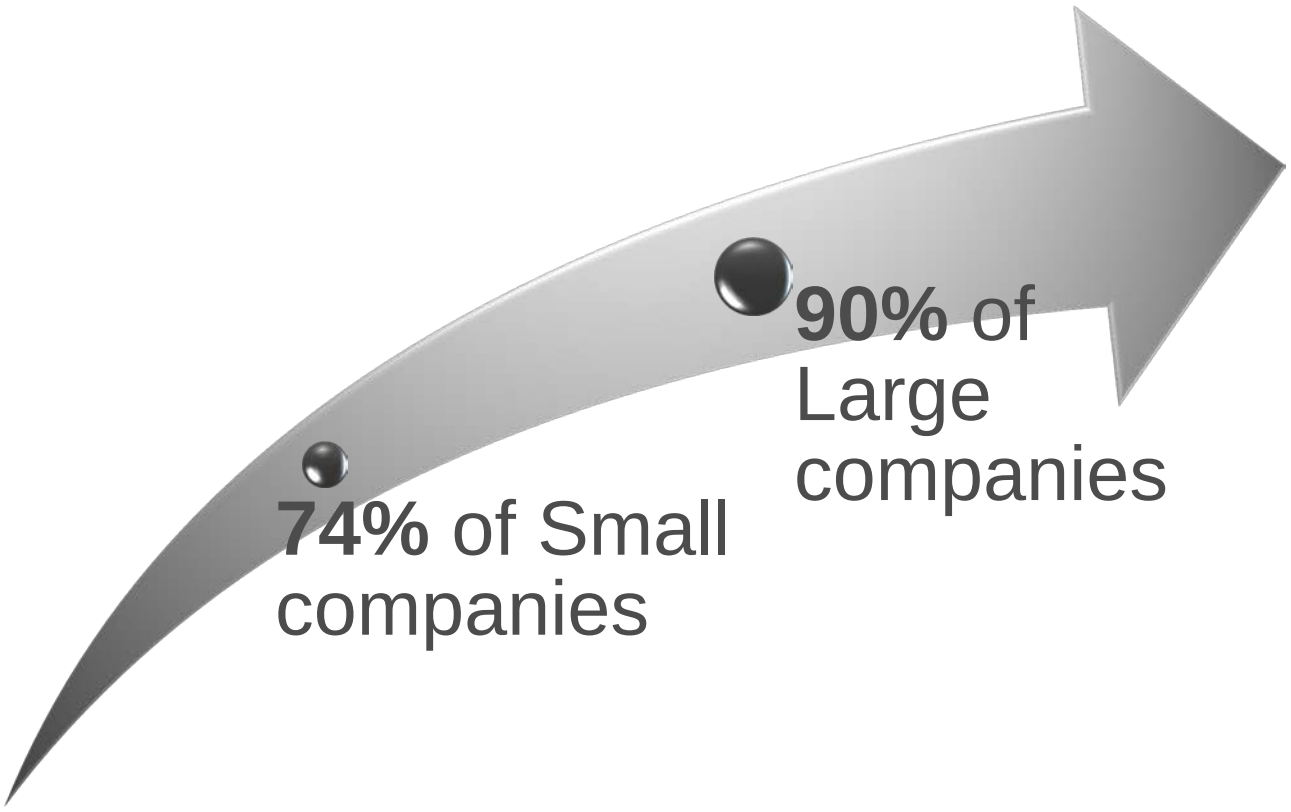
andreas@cnti.org.cy

Business in the Digital Era

- Internet changed the mentality of companies
- Online presence is mandatory
- Exposure to risks, threats

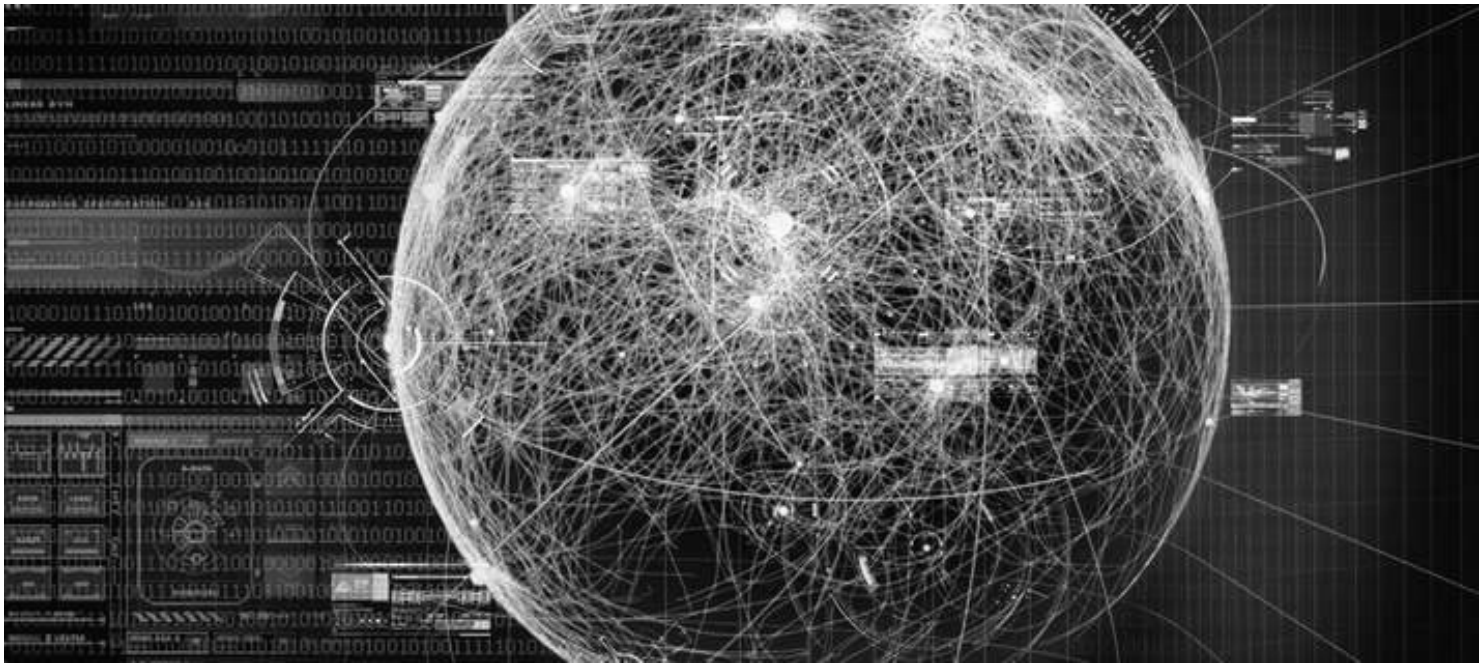
UK Information Security Breaches Survey (2015)

- Vast increase in incidents
- Top concern of companies
- What's the real picture?



Responding through technology

- Predominant attention on technology
  - Antivirus, breach detection systems, access control systems
- Are these measures effective? Why are companies still targeted and entrapped?



The human factor

- It is much easier to deceive an employee to give you access into the system than trying to hack the system

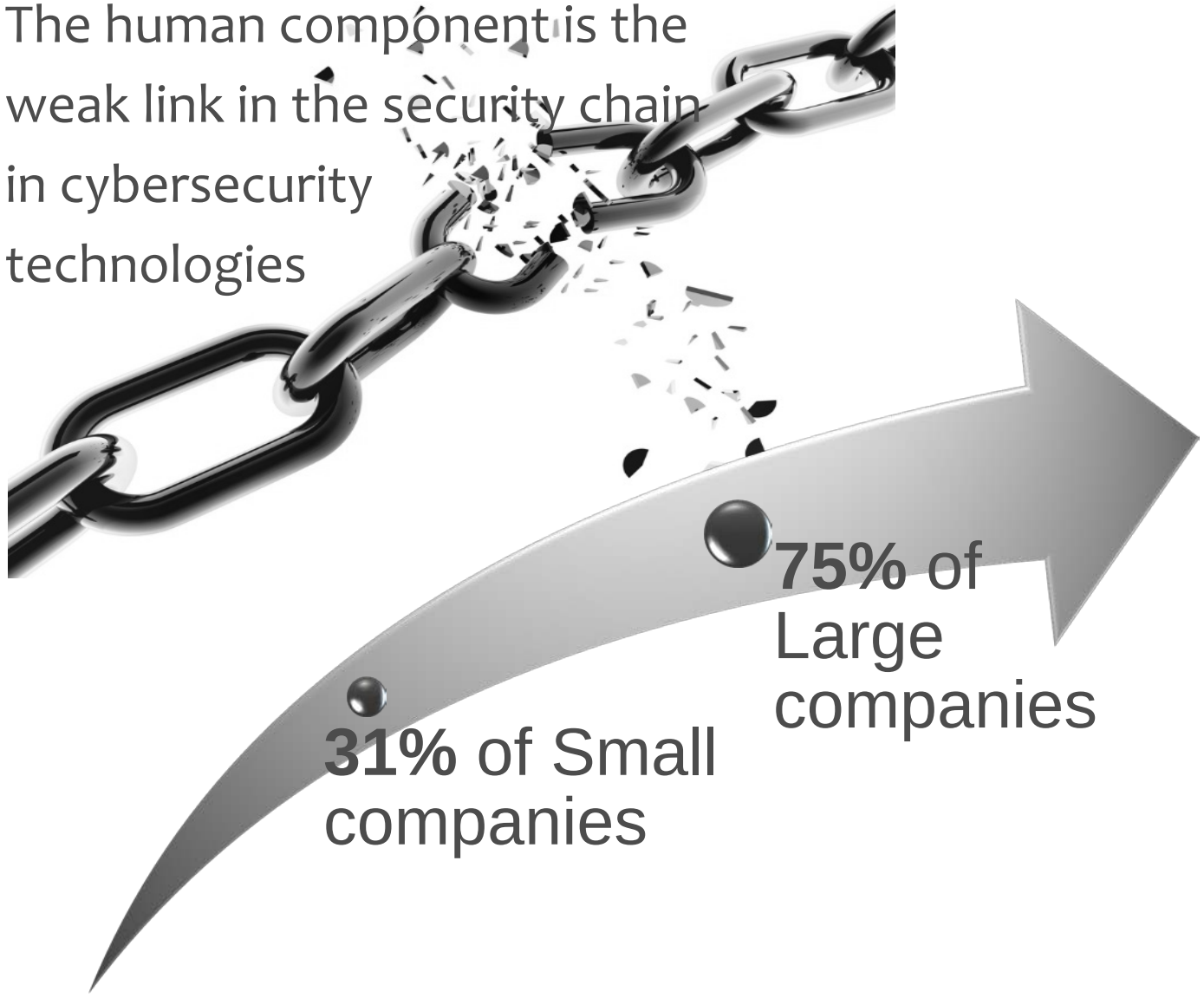
Technological knowledge and time to exploit the vulnerability of the system

VS

Sophisticated methods to exploit the vulnerability of the employee susceptible to curiosity

Incidents caused by human errors

The human component is the weak link in the security chain in cybersecurity technologies

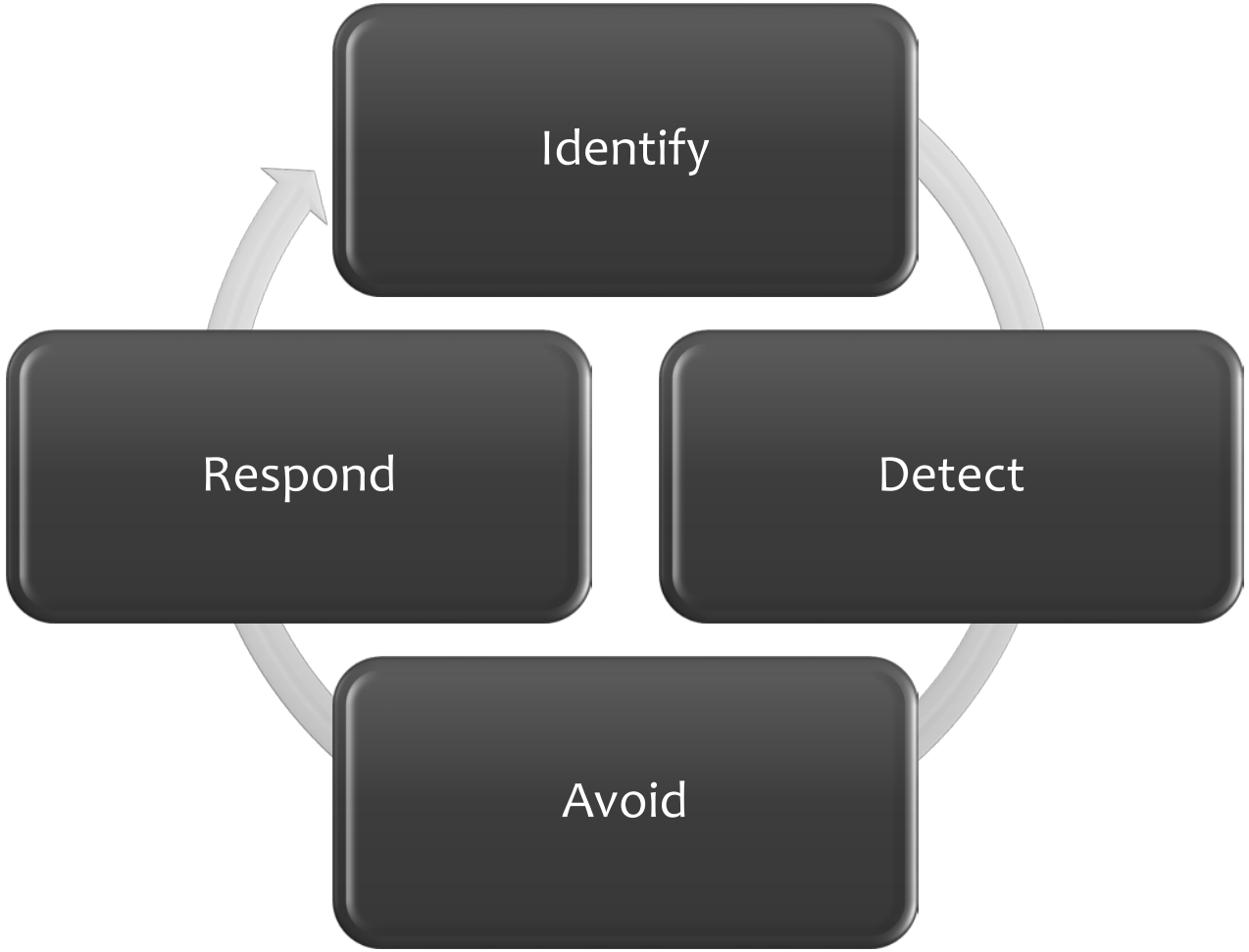


Towards a new Cybersecurity approach

- Technical security solutions cannot **solely** work effectively to safeguard the company
- Technological solutions together with a dynamic and intensive cybersecurity awareness

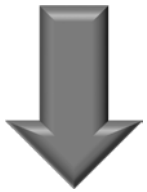
→ cybersecurity culture

Cybersecurity awareness training



Why cybersecurity awareness for SMB?

- Budget constraints
- Mentality “it will never happen to us because hackers go for the big fish”



- Failure to
  - understand that they are targets
  - comprehend the consequences of an attack
    - Financial loss, harm of reputation, termination of operations
  - understand the role of human factor in cyber incidents

Real Cases

- Malware attack executed through an attachment in an email from Amazon.com
- Cost $2,500

RICHMOND REGION TOURISM

- Employee clicks on an online advert
- A ransomware is installed on the computer
- 70,000 reports are locked
- Cost $500

SHERIFF DICKSON COUNTY EST. 1803 TN

Real Cases

- Ransomware in an email link
- 12,000 files encrypted
- Cost £3,000

MNH~platinum

total fleet solutions

"We were completely unprepared for a cyber breach simply due to a lack of awareness of the magnitude an attack of this type could have through mistakenly clicking a link in an email," says managing director Mark Hindle. "I am thankful that we had a lucky escape, in that I was able to retrieve the documents that are crucial to the running of the business, albeit at a price."

- Newsletter to 781 subscribers
- "TO" instead of "BCC"
- The names of the patients were leaked
- Fine £180,000
- New General Data Protection Regulation: security breach that leads to a compromise of customers' data can result to a **fine of up to €20 million of 4%** of the company's annual revenue

Concluding remarks & Cyprus

safer internet @cyberethics

Cyprus Cybercrime Center of Excellence

- Lack of awareness on cybersecurity and internet safety among businesses

CNTI

+

CYPRUS CHAMBER OF COMMERCE AND INDUSTRY

→ Development of targeted training modules for businesses

Thank you for your attention

Andreas Andreou (MSc, BA)

Cyprus Neuroscience & Technology Institute

andreas@cnti.org.cy