From Cybersecurity Awareness to Cybercrime fighting

Basie von Solms, Jaco du Toit, Elmarie Kritzinger

UNIVERSITY
OF
JOHANNESBURG

Adaption of a paper accepted for presentation at the HAISA conference in July in Kent

UNIVERSITY
OF
JOHANNESBURG

Headline Cyber Crime Statistics (June 2023)

- Around 236.1 million ransomware attacks occurred globally in the first half of 2022.
- 1 in 2 American internet users had their accounts breached in 2021.
- 39% of UK businesses reported suffering a cyber attack in 2022.
- 53.35 million US citizens were affected by cyber crime in the first half of 2022.
- In 2020, malware attacks increased by 358% compared to 2019.

https://aag-it.com/the-latest-cyber-crime-statistics

Cybersecurity budgets continue to increase despite economic headwinds (June 2023)

These may be challenging economic times but a survey of 200 CISO and IT decision-makers in the U.S. finds that

> well over half of the respondents (58%) reporting that cybersecurity budgets have increased, with 42% planning additional increases.

https://blog.barracuda.com/2023/06/19/cybersecurity-budgets-continue-to-increase-despite-economic-head

UNIVERSITY OF JOHANNESBURG

Something is very wrong somewhere!!

Cybercrime increases despite cybersecurity budgets increasing!!

My Premise 1 :

- Present Cybersecurity Awareness courses/approaches do not help to solve the cybercrime problem

UNIVERSITY
OF
JOHANNESBURG

My Premise 1 :

- **Present Cybersecurity Awareness courses/approaches do not help to solve the cybercrime problem**

- **Some comments**

  - to learn about cybersecurity
  - to learn how to protect my password
  - to learn about what phishing is
  - to see a lot of P/P slides
  - to not click on strange links in email messages
  - To not trust strange phone calls

- "It's Scary...It's Confusing...It's Dull"

https://www.usenix.org/system/files/conference/soups2018/soups2018-haney-perceptions.pdf

My Premise 2 : (based on looking back 50 years!!)

- Cybersecurity is all about Cybercrime
  - We use the wrong terminology
  - We should not make users ‘Cybersecurity Aware’
  - We should make them ‘Cybercrime fighters’
  - We should create a ‘cybercrime fighting workforce’

UNIVERSITY OF JOHANNESBURG

My Premise 3 :

- **The more users understand Cybersecurity as the ‘weapon’ to fight cybercrime, the more cybercrime will decrease**
  - **Every cyberrisk aware user who recognizes a cyberattack and do not react, prevents a cybercrime**

My Premise 4 :

- **A cybersecure end user (workforce) understands that fighting cybercrime to part of their daily job responsibility and help to protect the company and their jobs.**
  - ‘***Connect awareness to business benefits***’

- **Companies and researchers (across the globe) are searching for new ways and approaches to make (their) end users more cyber aware.**

- **This presentation discusses three ways to try to achieve that – actually four!!**

Time line – Data Security/Data Protection

1970

- Mainframes
- Centralized databases
- Central processing
- Dumb terminals
- Dedicated communication
- Few terminal endusers (Data input)

- **Data (Information) Security a very small problem**

2023

- Distributed servers
- Distributed databases
- Client/Server processing, distributed processing
- Powerful intelligent workstation computers
- Internet/Cyberspace communications
- Everybody with a computer is an enduser
- Cloud
- BYOD

- **Data (Cyber) Security a massive problem**
- **Cybercrime**

UNIVERSITY OF JOHANNESBURG

Four approaches

- **The 1970 approach**

- **The ‘Fighter’ approach**, is taken from the area of firefighting, where employees are trained to fight a fire in an emergency.

- **‘Ownership’ approach**, is from the operational technology (OT) area where machine operators are trained to take ownership of their machines and safely operate their machines.

- **‘Workplace’ approach**, is taken from the area of workplace training where being c awareness is seen as a part of a secure workplace.

The ‘Fighter’ approach

- Area of firefighting, where employees are trained to fight a fire in an emergency.

- Application : This approach is based on the ideal situation that every end user understands that he or she is probably in the aim of the cybercriminal to launch a cyberattack on the company.

- The ideal situation that every end user will accept that he/she is a (cyber-crime) fighter to prevent cybercrime and to protect the company against any damage from cyberattacks and resulting cybercrime.

The ‘Fighter’ approach

- Firefighting course (NOT ‘Fire-awaress course’)
  - How to identify fire hazards and report
  - How to handle a fire extinguisher
  - Understand their responsibility and involvement in preventing fires for the benefit of the whole company and specifically their own jobs

The ‘Fighter’ approach

ApplicationCybercrime fighter approach

- How to identify cyber attacks and report
- How to handle their workstation is a secure manner
- Understand their responsibility and involvement in preventing cyberattacks for the benefit od the whole company and specifically their own jobs

The ‘Fighter’ approach

- **Premise** : Every end user who does not fall for a cyberattack, prevents a cybercrime
- **Example :** BEC case in South Africa

‘Ownership’ approach (TPM/OT)

- Total Productive Maintenance (TPM) combines the traditionally practice of preventive maintenance with total quality control and total employee involvement to create a culture where operators develop ownership of their equipment, and become full partners with maintenance, engineering and management to assure that equipment operates properly every day.

- Operational technology (OT) area where machine operators are trained to take ownership of their machines and safely operate their machines.

- Users understand that the machine they operates is essential for the health of the company to prevent interruptions in manufacturing and bad products

‘Ownership’ approach (OT)

Application

Users understand that their workstations are essential for the health of the company to prevent cyber incidents

- They are responsible to use their workstations in a secure and responsible way

- They will take extra responsibility for their computing devices (workstations) to protect the workstation and ensure that the work-station is not used as an instrument to cyber attack the company

The ‘Workplace’ Approach

- Based on the usual health and safety training that all employees get in any company – in many cases such training is required by law.
- In general terms, the purpose of health and safety training can be seen as providing for the safety and health of persons at work in connection with the use of machinery
- Based on the ideal situation that every end user will feel safe and secure in his or her workplace environment.
- Help prevent legal and insurance claims
- Health and safety training is important because it equips workers with the knowledge of how to perform their duties correctly and in the most secure and safe way possible
- It can be characterised as ‘***the way we do things around here***’

The 'Workplace' Approach

Application

- More health and safety courses now include online safety and cyber security
- Emphasizes the benefit of online safety and cyber security as a benefit to all – the company and co-workers.
- Creates a sense of personal responsibility and view security and safety as relevant to their day-to-day lives.

Conclusion

- None of these approaches had been ‘proven’ in any way

- It remains conceptual ideas which can possibly change the end user’s understanding of his/her role

- These approaches can all help to change the mindset of end users in creating a more cyber risk aware workforce

Conclusion

Challenge:

We as academics and practitioners must find new ways and models to really create a cyberrisk aware workforce

TC 8/TC 11

Factsheet 2021-2022 TC-8.11/11.13 Information Systems Security Research Aims and scope (last reconfirmed1: 2009; October 2013) The aim of the working group is the creation, dissemination, and preservation of well-formed research about information systems security

Change the mindset of the enduser to see such training as part of becoming a better cybercrime fighter realizing that cybersecurity is not an add-on but an integral component of your job

IF not : Back to 1970!!

Thanks

basievs@uj.ac.za

UNIVERSITY OF JOHANNESBURG