Cybersecurity Governance – it is everybody's responsibility

Prof Basie von Solms
University of Johannesburg
basievs@uj.ac.za

PURCHASING CONSORTIUM SOUTHERN AFRICA NPC
ISO 9001:2015 certified company

UNIVERSITY OF JOHANNESBURG

Let us look at some major recent hacks and data leaks in SA

- **Transunion** - >60 million personal recoreds of SA leaked, including info on the SP
  - **How** : enduser was negligent and used ‘password’ as password

- **SA University** – 100 million lost through a cyber attack, but most recovered
  - **How** – enduser did not enforce proper cybersecurity

- **Colonial Pipeline USA** –
  - **How** - re-use of an old password

- **Dis-Chem**
  - **How** - data hack at one of its third-party service providers

- **CISCO (May 2022)**
  - **How -** through a successful phishing attempt of an employee's personal Google account.

Let us look at some major recent hacks and data leaks in SA (cont..)

- Companies are spending millions on technical solutions to mitigate cyberattacks
- BUT .. Cyberattacks keep increasing
- Clearly technical solutions alone do not work
- Why?
- Common component in many of these hacks above
  - User-error/lack of cyber risk awareness
  - 88% of Data Breaches are Caused by Human Error

    https://blog.knowbe4.com/alert-new-stanford-research-88-of-data-breaches-are-caused-by-human-error

Let us look at some major recent hacks and data leaks in SA (cont..)

- **88% of Data Breaches are Caused by Human Error**

  https://blog.knowbe4.com/alert-new-stanford-research-88-of-data-breaches-are-caused-by-human-error

- **We have to up our efforts as far as cyber protection from the human dimension**

Let us look a little closer at this Human Dimension

- Cybercriminals are going for the weakest link (at the moment) – the end user (human side)
- The end user has become as important, or even more important,
  than the security staff in cyber-protecting the company.
- Cyberattacks cannot be thwarted by technical means alone
- The end user is an essential component of a company's cyber protection
- Every cyberattack which the end user recognises and do not fall for, most probably prevents a
  cybercrime in the company
- The most effective way to reduce cyber security risk within your organization is
  to address the human link in that chain.

https://terranovasecurity.com/security-awareness-training/

PURCHASING CONSORTIUM SOUTHERN AFRICA NPC
ISO 9001:2015 certified company

UNIVERSITY OF JOHANNESBURG

Let us look a little closer at this Human Dimension (cont ..)

https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

- … the data clearly and consistently shows that employees are the greatest (cyber) vulnerability of any organization.

- .. the largest “attack surface” of the organization is you and me—the people who perform common functions:
  - Leadership, Planning, and Governance,
  - Sales, Marketing, and Communications
  - Facilities, Physical Systems, and Operations
  - Finance and Administration; Human Resources;
  - Legal and Compliance; and routine Information Technology operations.

- Each worker in the company, from the newest employee to the chief executive, holds the power to harm or to help and to weaken or strengthen the organization’s security posture.

- **Therefore, cybersecurity is everyone’s job**

PURCHASING CONSORTIUM SOUTHERN AFRICA NPC
ISO 9001:2015 certified company

UNIVERSITY OF JOHANNESBURG

Let us look a little closer at this Human Dimension (cont ..)

Core message

- Each worker in the company, from the newest employee to the **Chair of the Board/Council**, holds the power to harm or to help and to weaken or strengthen the organization's security posture.

How can an end user harm the organization's cyber posture?

PURCHASING CONSORTIUM SOUTHERN AFRICA NPC
ISO 9001:2015 certified company

UNIVERSITY OF JOHANNESBURG

How can end users harm or ‘cyber sink’ a company?

- Phishing attacks
  - Infected email attachments
- Choosing a bad password
- Sharing login info
- Visiting dubious websites
- BEC attacks

- **Consequences**
  - Ransomware – lose control over your data
  - Lose money

- **Legal consequences**
  - POPI
  - Cybercrime Act

So, who are the role players in Cybersecurity Governance and Cybersecurity Resilience?

Something on Cybersecurity Governance and Cybersecurity Resilience

- Cybersecurity Governance is a core component of good Corporate Governance
- A very general definition of Corporate Governance is to keep the company safe and resilient in all areas
- A very general definition of Cybersecurity Governance is to keep the company safe and resilient as far as cyberattacks are concerned
- **Top management has the oversight responsibility as far as Corporate and Cybersecurity Governance is concerned**
- **However, top management are also end users exposed to cyberattacks.**

So, who are the role players in Cybersecurity Governance and Cybersecurity Resilience?

- **Everybody!**
  - Board/Council
  - Executive Management
  - Managers
  - Academics
  - All end users (every employee in the company)
    - Cyberattacks are more and more directed at the end user
  - Third party supplies

- **Why?**
  - Protecting a company against cyber threats and cyberattacks (making the company cyber resilient) must involve everybody in the company

- **How?**
  - By ensuring that every end user is a cyber-risk aware cybercrime fighters (a 'Human Firewall') that helps protect them and their enterprises on the front line of cyber crime.

The real Challenge to make and keep a company cyber resilient

- Create a Cybersecurity culture throughout the company
- Let every end user understand he/she is part of the cyber protection of the company
- Create a Cyber risk-aware workforce – from the highest level right through to be lowest level
- Make every employee a Cybercrime Fighter
- Create a Human Firewall
- **How?**
  - **Empower every end user to be a cybercrime fighter**

Empower the End user to be a cybercrime fighter

- Every worker should be empowered, trained and skilled so that every worker becomes a protection wall against cyberattacks – create a Cybercrime Risk-aware workforce

- Empowering workers to such a level, where they understand they actually fight cybercrime, is much more than just exposing them to a Cybersecurity Awareness course

- It should be the purpose to let every employee understand that he or she is a cybercrime fighter helping to defend the company!

- For that reason, it must be considered that maybe, specifically in terms of the 4th Industrial Revolution,

    - The term Cybersecurity Awareness (CSA) (programme) is outdated

    - The term Cybercrime Fighting and Prevention (CCFP) (programme) describes the purpose better

Cybersecurity Awareness programs vs Cybercrime Fighting and Prevention programs

- **ALL** Employees should be told they are attending Cybercrime Fighting and Prevention programs to do precisely that – preparing them to become cybercrime fighters to help prevent and fight cybercrime.
- Firefighting Training vs Firefighting Awareness
- Must be practical

purco
PURCHASING CONSORTIUM SOUTHERN AFRICA NPC
ISO 9001:2015 certified company

UNIVERSITY OF JOHANNESBURG

Possible ways to create a Cyber-risk aware workforce

- Confront end users constantly with simulated cyber attacks
  - Simulated phishing attacks
  - Simulated infected emails
  - Simulated phone calls

Summary

- A cybercrime fighting and prevention program needs to be integrated into end users' daily work (including top management).
- Practical and continuous
- Researchers and designers need to think of clever ways to establish a cyber risk-aware workforce.

What is the message?

- Cyber-aware workforce will result in a decrease of Cybercrime in a company (country)
- Empower and convince all employees that
  - they are actually cybercrime fighters
  - They are part of the cyber defence structure of the company

Conclusion

- Move away from the traditional terminology of Cybersecurity Awareness programs, and rather refer to Cybercrime Fighting and Prevention programs - **pro-active vs reactive**

- It must be accepted that employees and end users are actually the most essential cybercrime fighters in the company as they actually fight every day in the front trenches.

- Everything must be done to make their cybercrime fighting and prevention skills as sharp as possible

Thanks

basievs@uj.ac.za

purco
PURCHASING CONSORTIUM
SOUTHERN AFRICA NPC
ISO 9001:2015 certified company

UNIVERSITY OF JOHANNESBURG