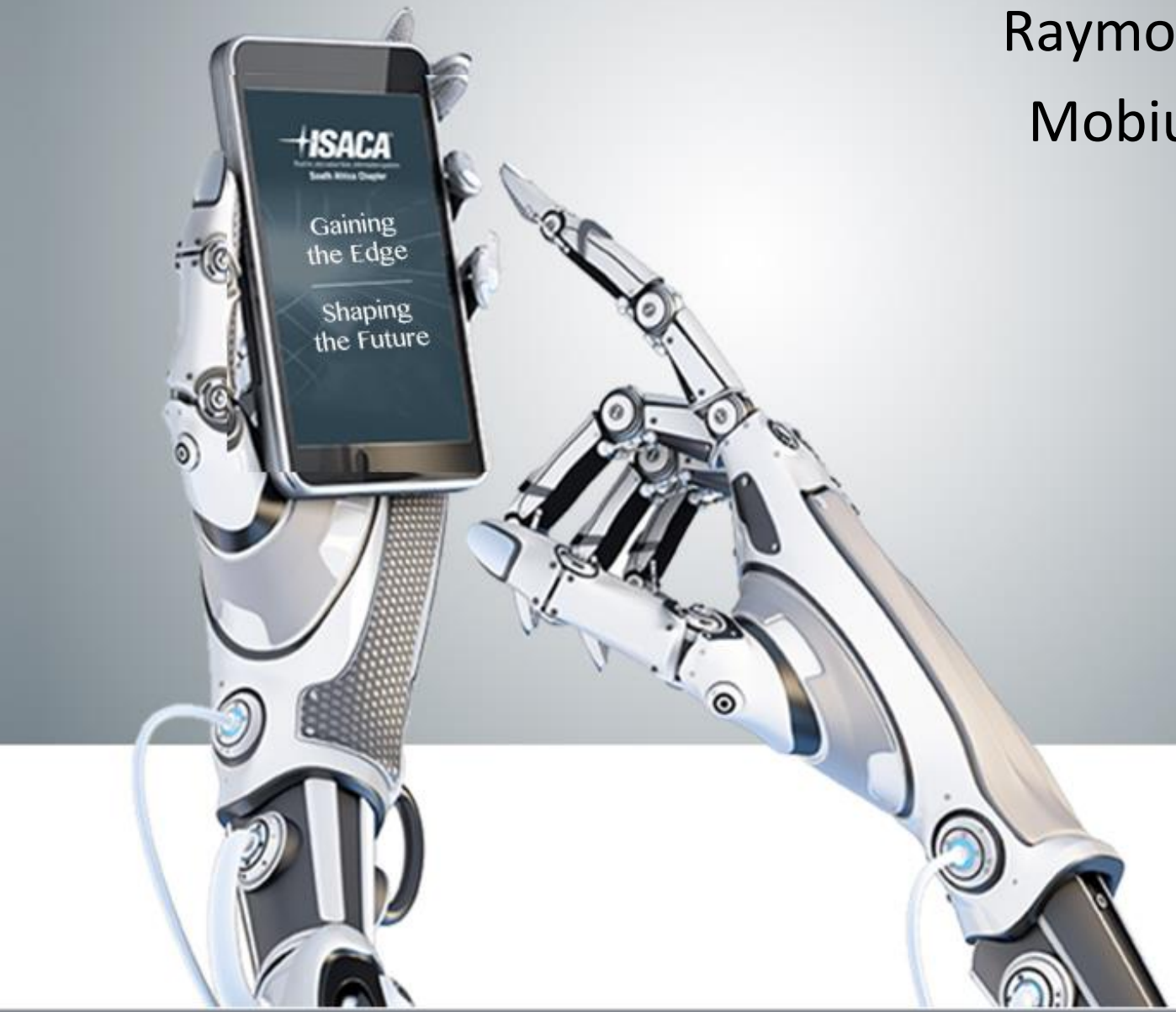
Vulnerability management lifecycle

Raymond du Plessis

Mobius Consulting



ISACA®

Trust in, and value from, information systems

South Africa Chapter

ISACA
Trust in, and value from, information systems
South Africa Chapter

About the speaker

- 11 years of Information Security experience, and many more years in IT
- All the usual credentials
- Experience from both sides
  - external perspective - solution provider, consultant, assessor
  - internal perspective – risk, management, operations
- Passionate about
  - pragmatic approaches
  - effective information security

ISACA
Trust in, and value from, information systems
South Africa Chapter

Topic context

Effective reduction of technology based vulnerabilities through governance and improved vulnerability management practices.

- Typical failures
- Going beyond scanning and reporting
- Closing the loop by improving testing
- Governance aspects

ISACA
Trust in, and value from, information systems
South Africa Chapter

Usual response to vulnerabilities…

- Assess (scan)
- Report
- Pass on

And every now and again …

- Re-asses (follow up scan)

And on very special occasions …

- Test (penetration testing)

ISACA
Trust in, and value from, information systems
South Africa Chapter

Usual response to vulnerabilities…

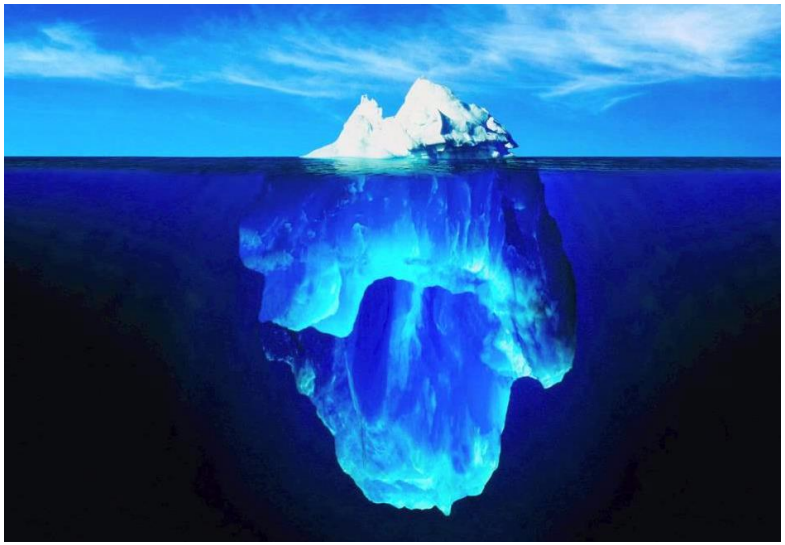
…. results in a false sense of security and breaches are still occurring.

ISACA
Trust in, and value from, information systems
South Africa Chapter

We need a more holistic approach …

- We need to consider
  - all types of vulnerabilities
  - going beyond running scans and producing reports
  - using more realistic testing methods
  - improving vulnerability governance

Vulnerability practices need to broaden in scope and maturity



#isacazaconf

ISACAZA @ISACAZA ISACA South Africa

ISACA
Trust in, and value from, information systems
South Africa Chapter

… what “other” vulnerabilities ?

Cybercriminals exploit technology and infrastructure vulnerabilities to gain control and access, but missing patches and misconfigurations are not the only way in ….

- Coding flaws
- Security design flaws
- Privileged access - the golden ticket
- Underlying virtual technology vulnerabilities
- Unprotected data
- Targeted social engineering attacks against custodians
- Physical access

ISACA
Trust in, and value from, information systems
South Africa Chapter

Testing needs to be extended

Over and above technology vulnerability scanning and penetration testing, what about ….

- Privileged access assessment
- Sophisticated social engineering testing against custodians
- Code flaw testing
- Data security testing
- Physical access testing

… and ultimately making use of attack path mapping and attack path testing

ISACA
Trust in, and value from, information systems
South Africa Chapter

And governance ?

Governance needs to ensure a more holistic approach is adopted to counter modern day sophisticated attack attempts

- Update policies, standards and practices inline with new threats
- Ensure all vulnerability types are considered
- Ensure more holistic and realistic testing
- Identifying and actually addressing root causes of vulnerabilities
- Security capacity and capability - people, process, technology
- Roles and responsibilities

- Measuring effectiveness

ISACA
Trust in, and value from, information systems
South Africa Chapter

*"The ultimate goal of vulnerability management is to **effectively** improve the security posture of the organisation"*

Thank you – any questions ?

#isacazaconf

ISACAZA @ISACAZA ISACA South Africa