University of Fort Hare

Together in Excellence

Information Security and the Dark Side of Trust!

By Stephen Flowerday

Professorial Inaugural Address

7th August 2013

Lecture Outline

- Trust and Risk
- Security
- Information Age
- Information Systems & Technology
- Paradigm Shift
- The Internet
- Information Security (threats, vulnerabilities…)
- The Future
- Conclusion

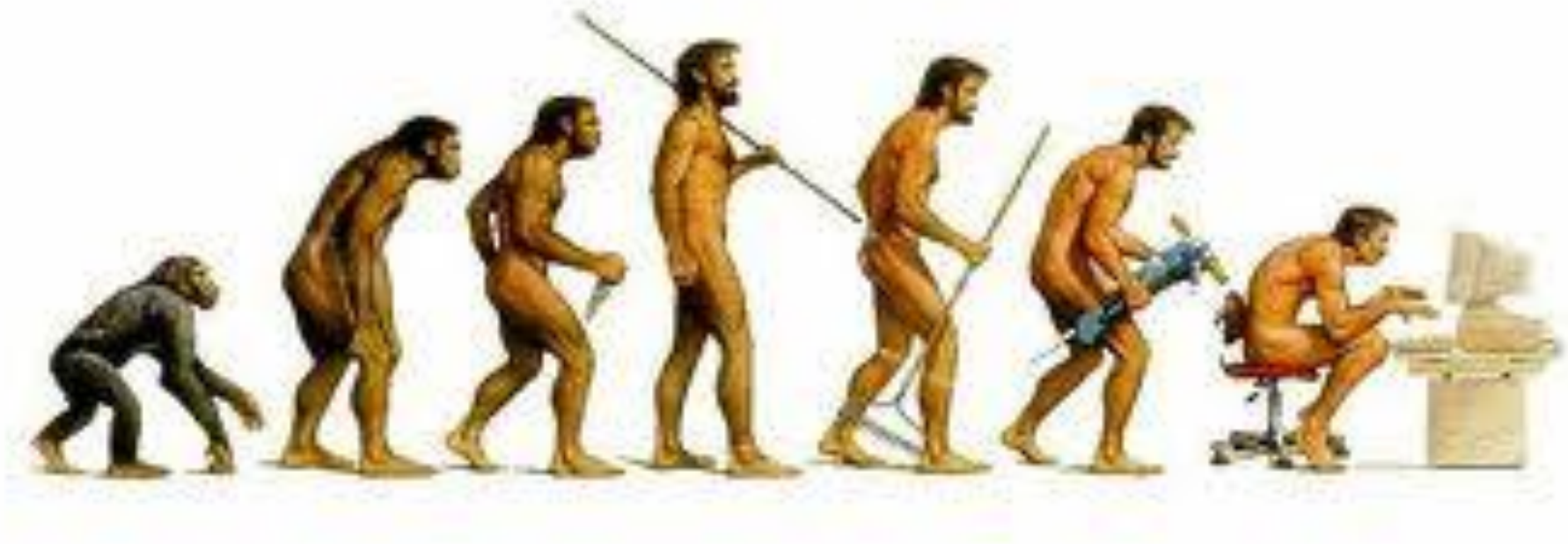
Trust & Risk


DARK SIDE
You will join us, or die!

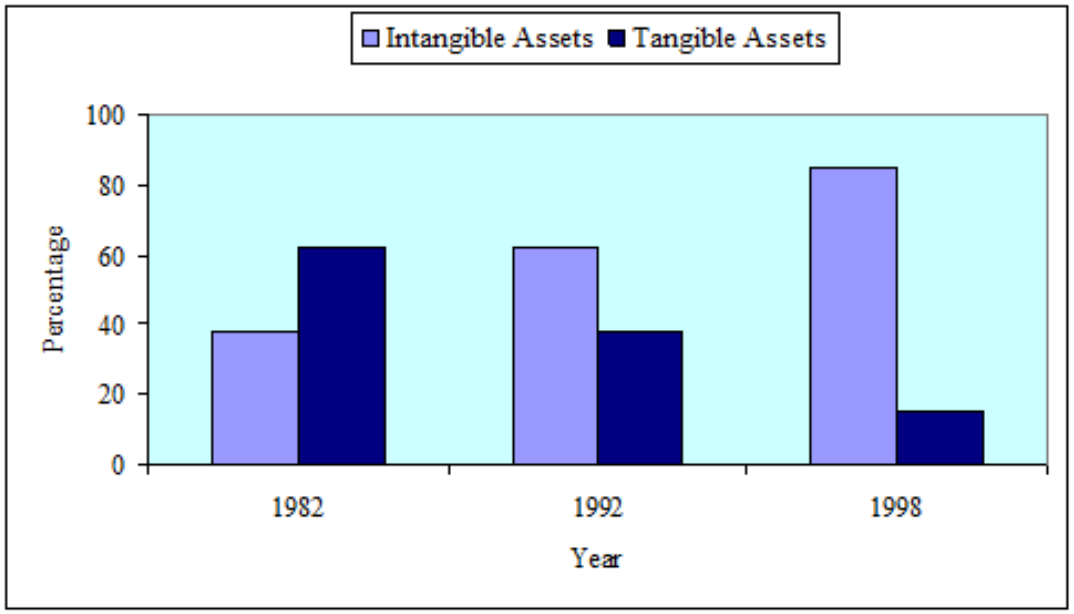
Security Forces (and individual security)

Information Age

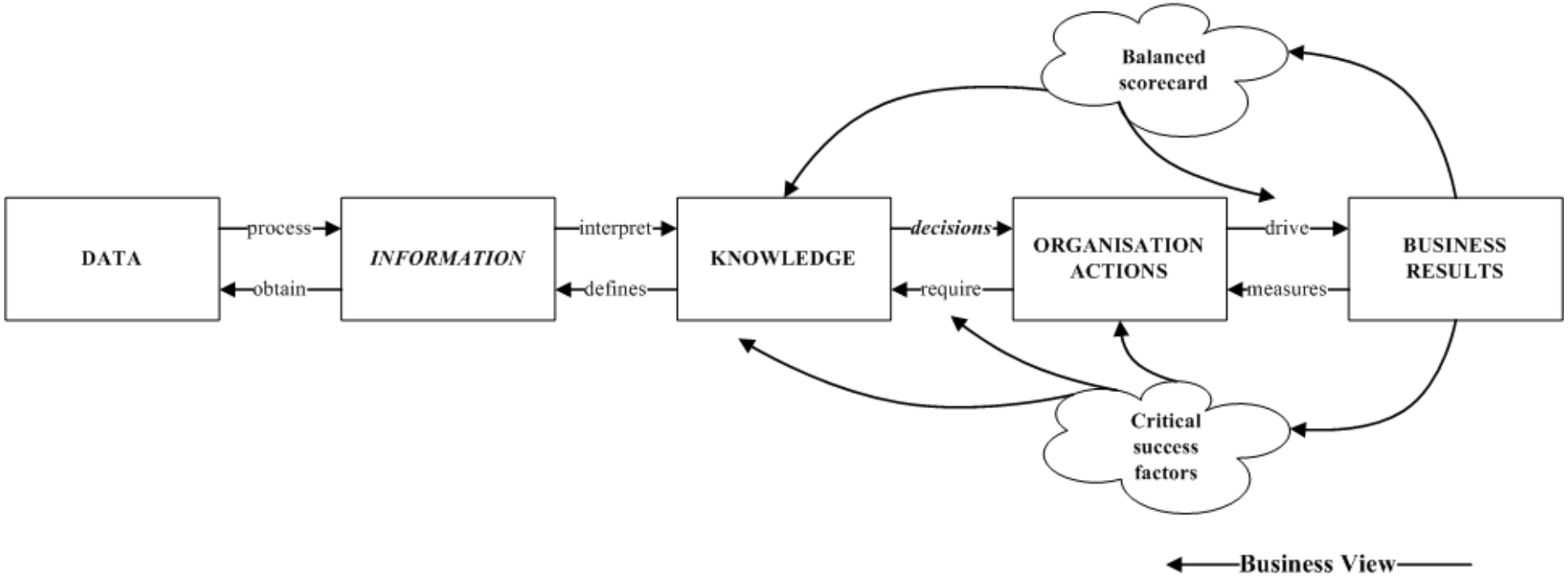
(note the weapons and tools of advancement)



What is Information?



Technology View



Business View

Information Systems

Server Farms

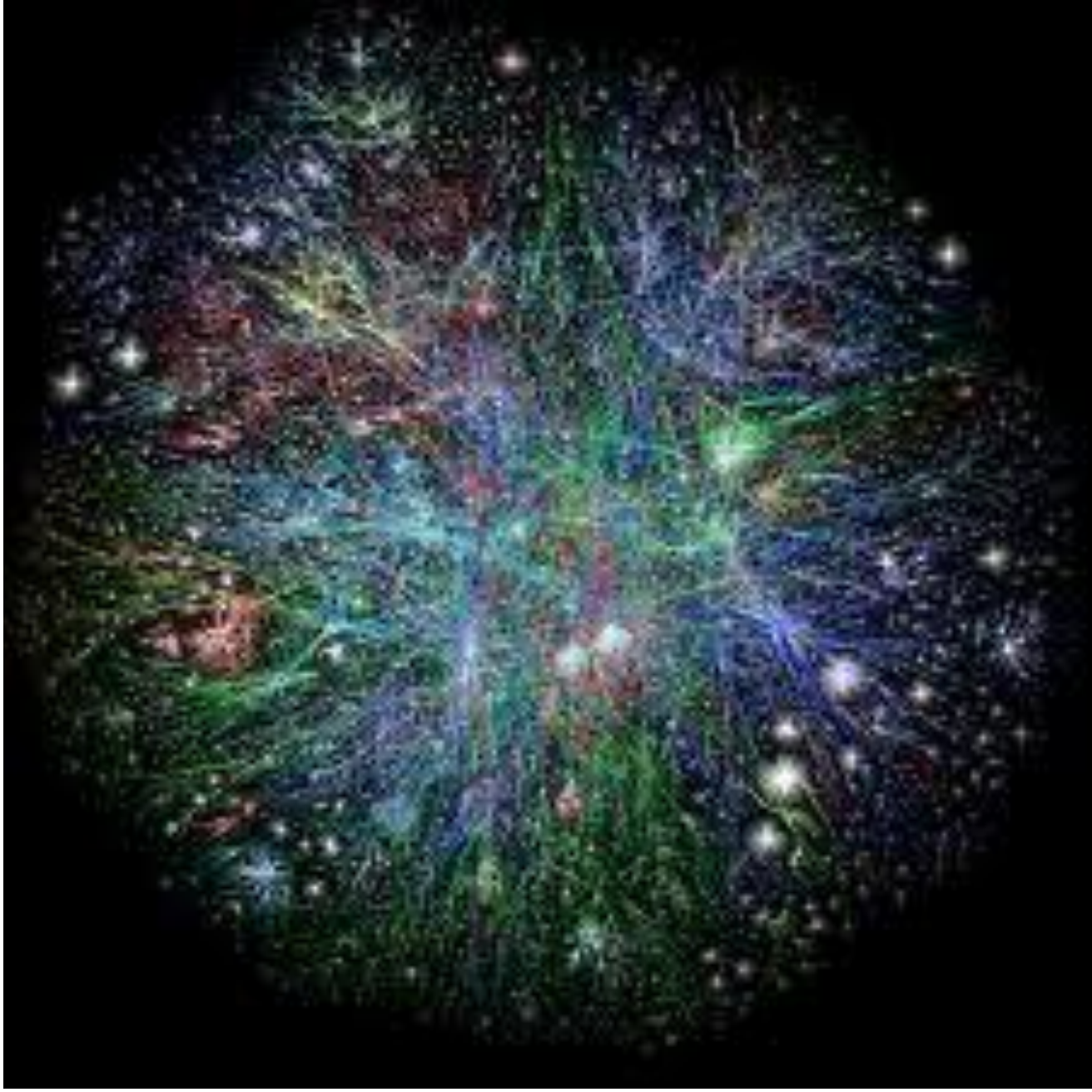
Paradigm Shift

- They were “Closed” but are now Open Systems!
- They were Complicated but they are now Complex Systems!

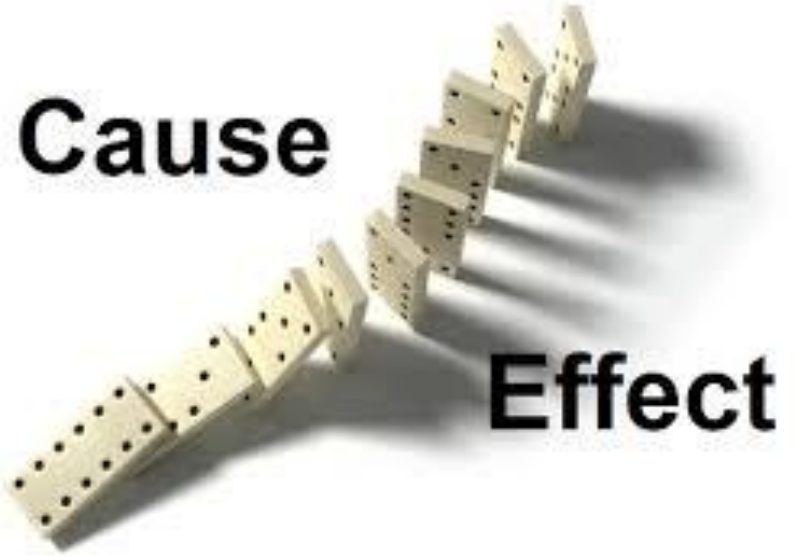
The way we used to plan and predict is no longer sufficient….

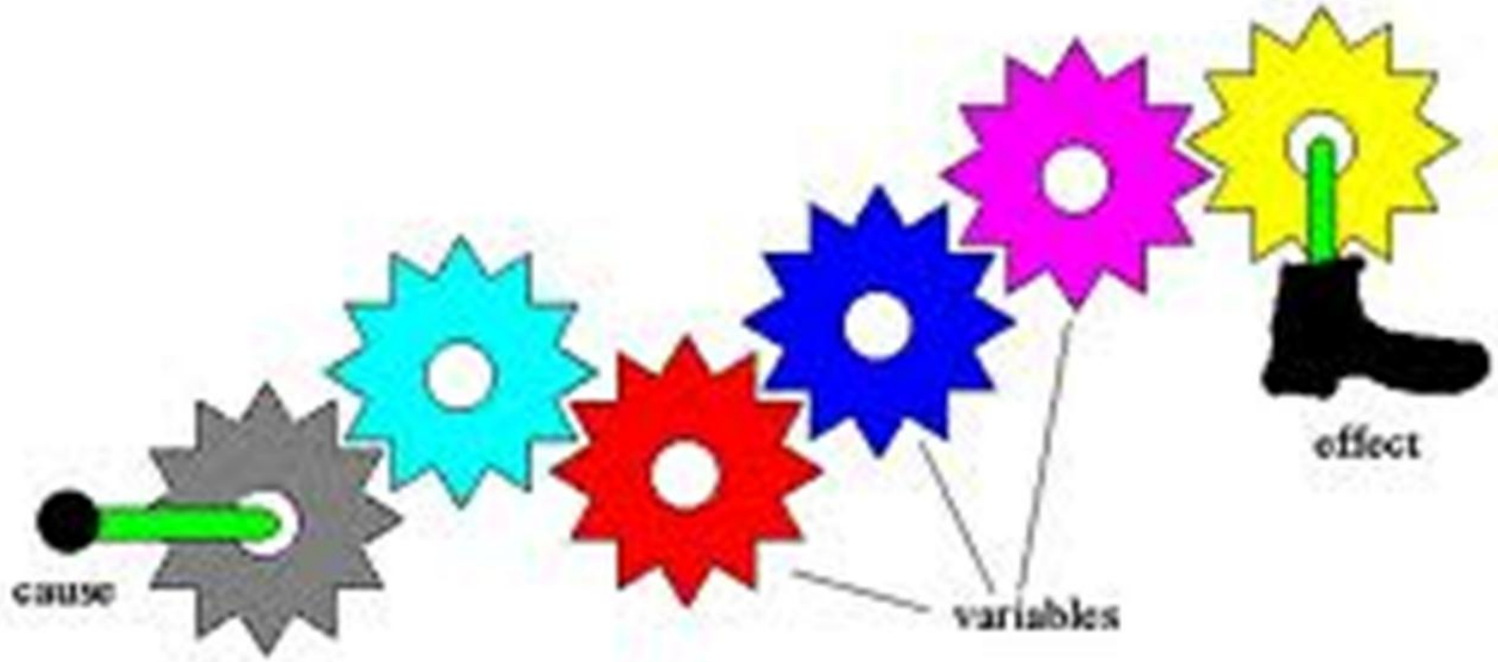
Closed System (more control)

Open System
(the internet)

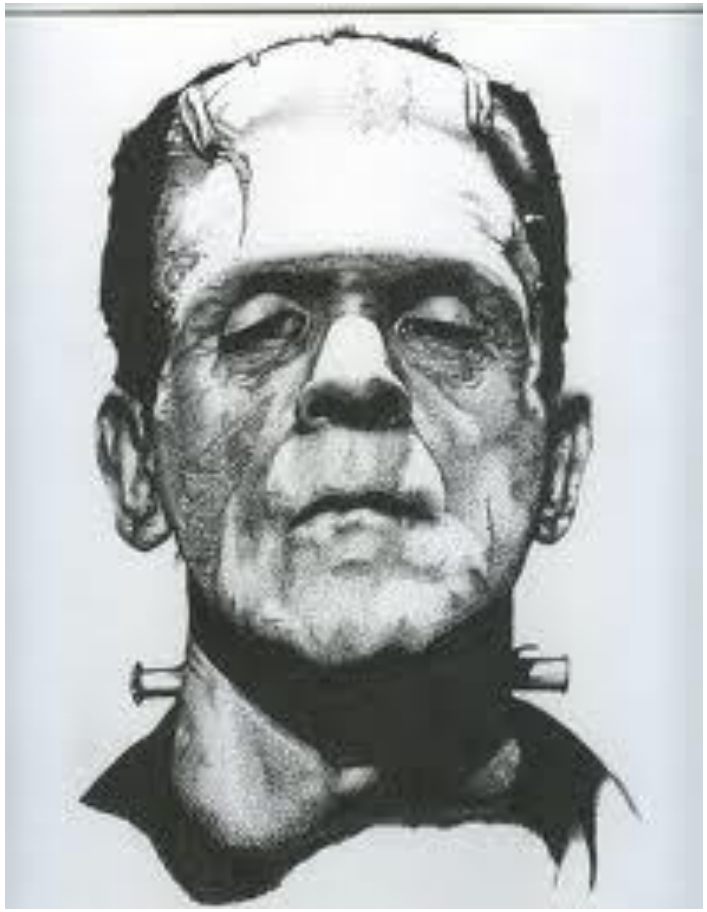


Determinism

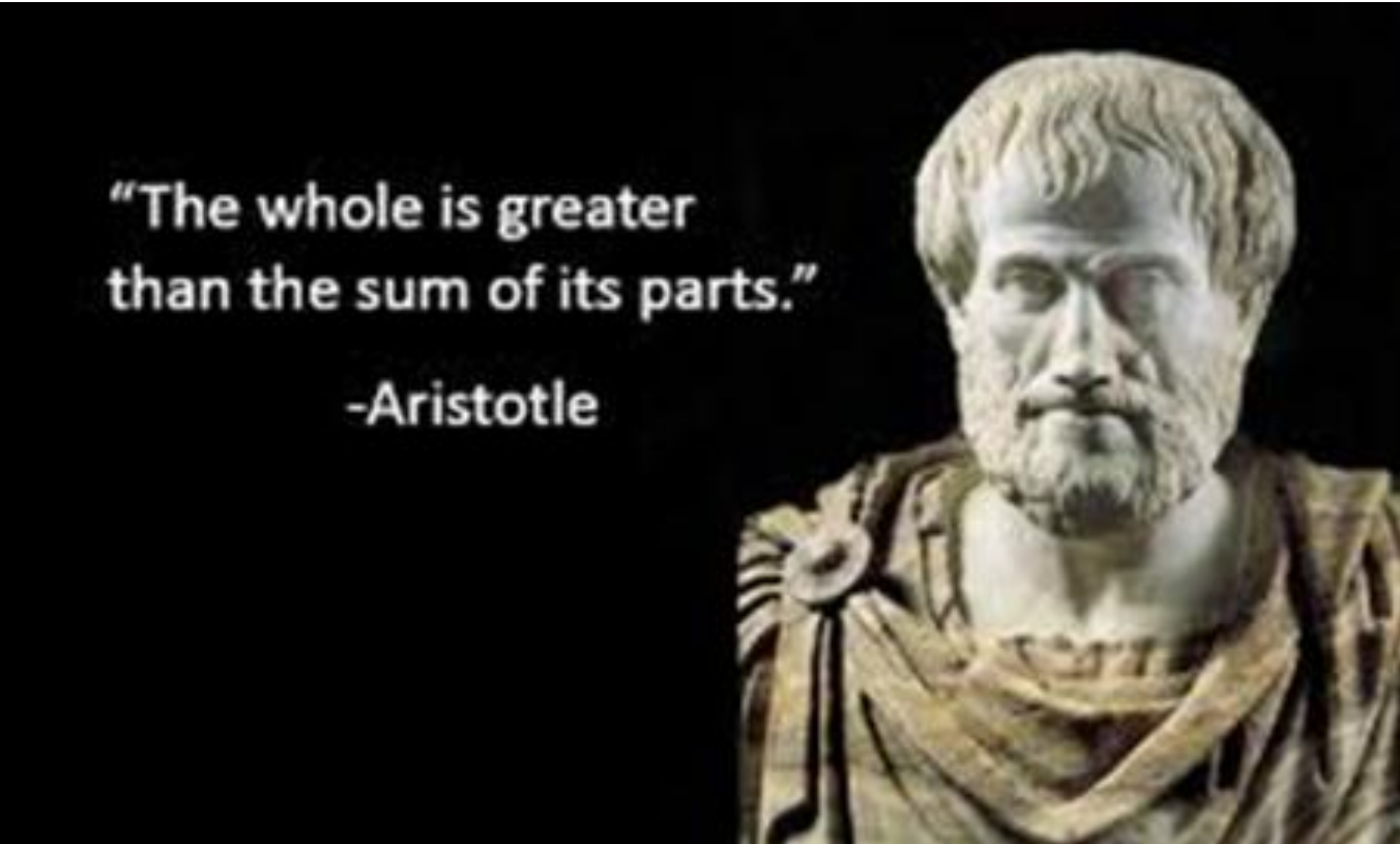




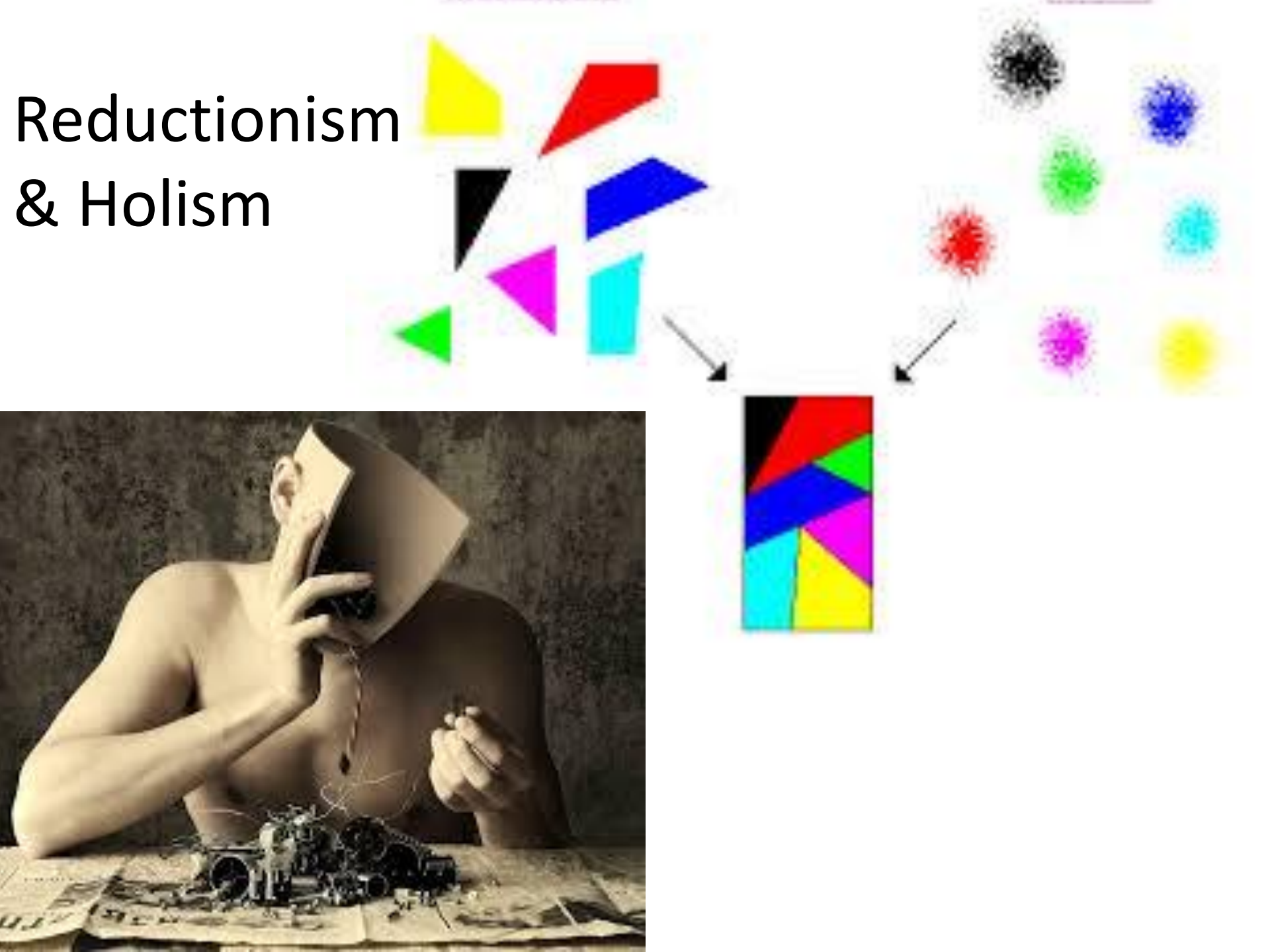
Reductionism



Holism (emergent property)



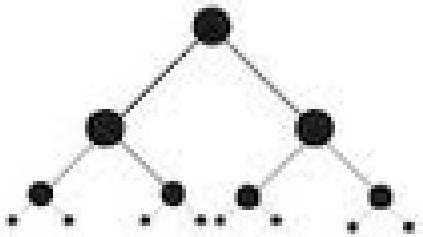
Reductionism & Holism



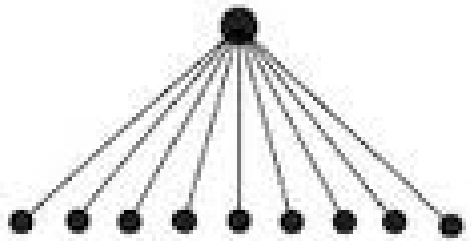
ATOMS AND PARTICLES BEHAVE IN DETERMINISTIC WAYS, AND OUR BRAIN IS MADE OF ATOMS AND PARTIC

HOW CAN FREE WILL EXIST?

Complex Environment



complex



complicated

(W)Holism

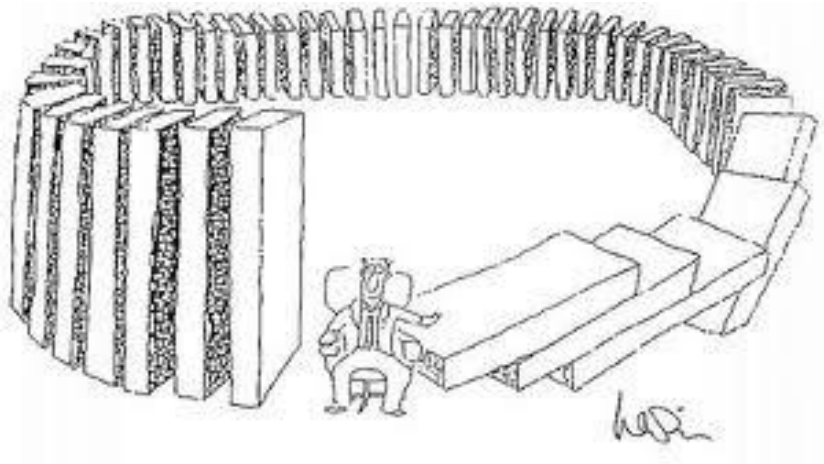
- The whole is greater than the sum of its parts
- Increased focus on the relationships between the parts
- Holism
- “Relativity”
- General Systems Theory
- Living Systems Theory
- Information Systems
- System of Controls (information security)
- Increased Trust, Risk and Uncertainty Reduced

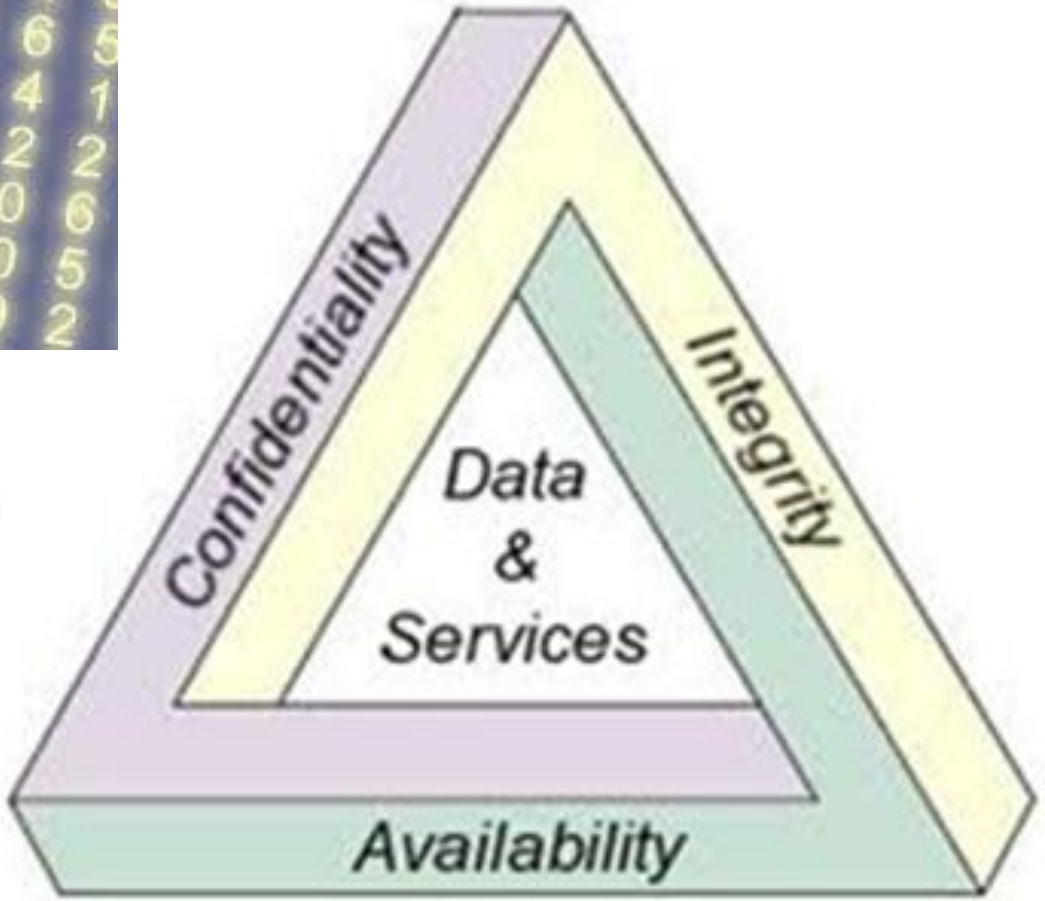
Information Security

- Military Principles (different tools)
- Information Age (new rules e.g. anonymous nature of threats…)
- Complex Environment (determinism incomplete)
- Emergent Property from the Sum of the Parts is Information Security as a Whole (reductionism incomplete)

What Must Be Protected?

Information of Organisations and of People!

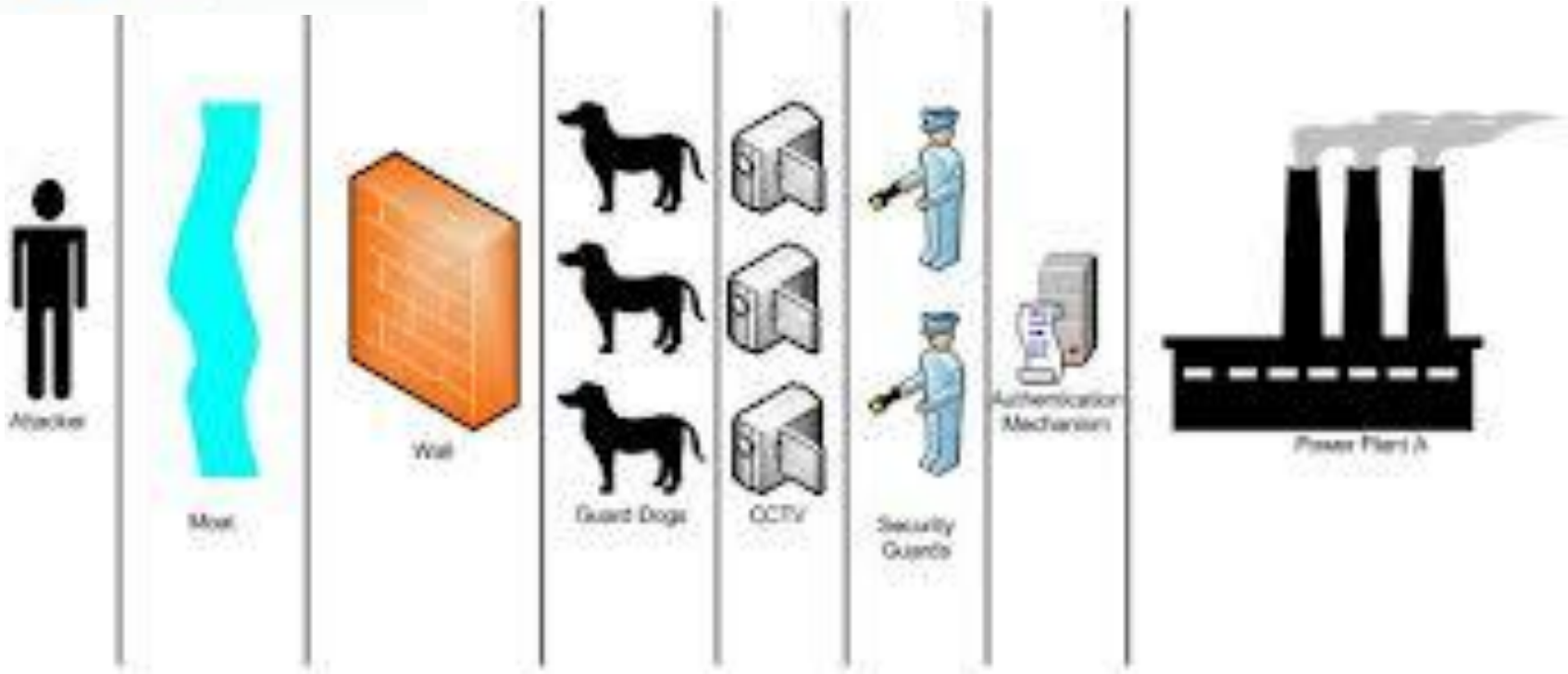




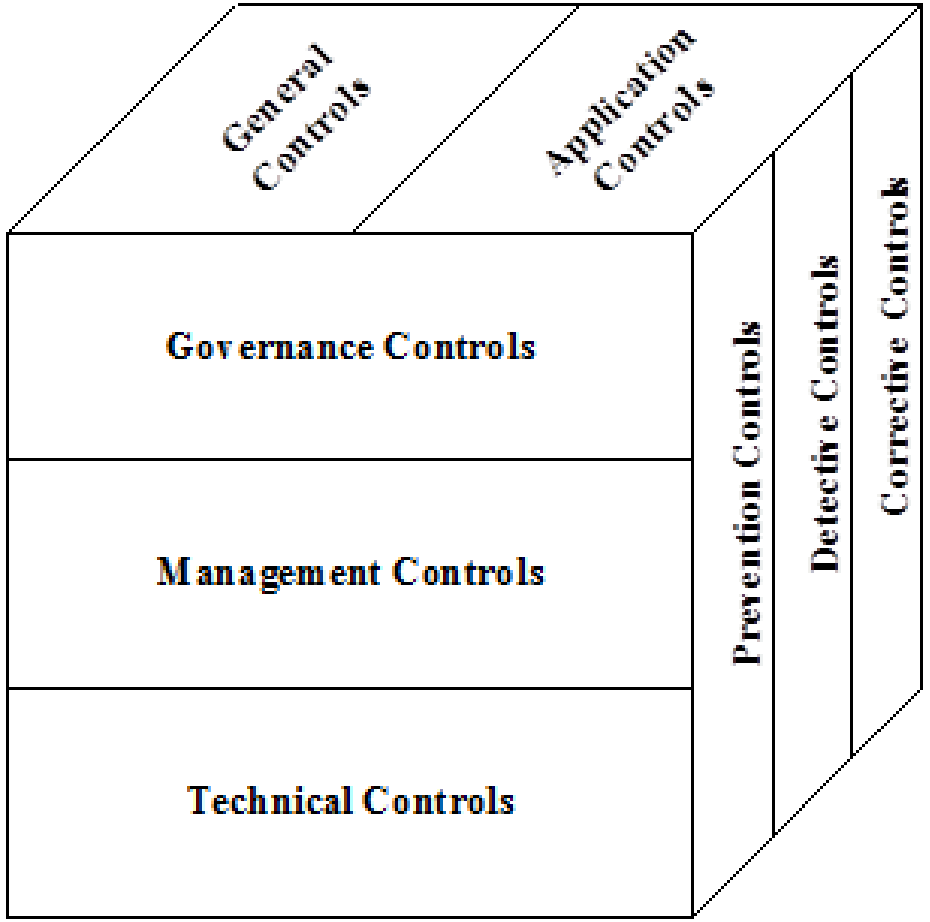
Information Security: All or Nothing!

Determine Asset Value: is it worth protecting?

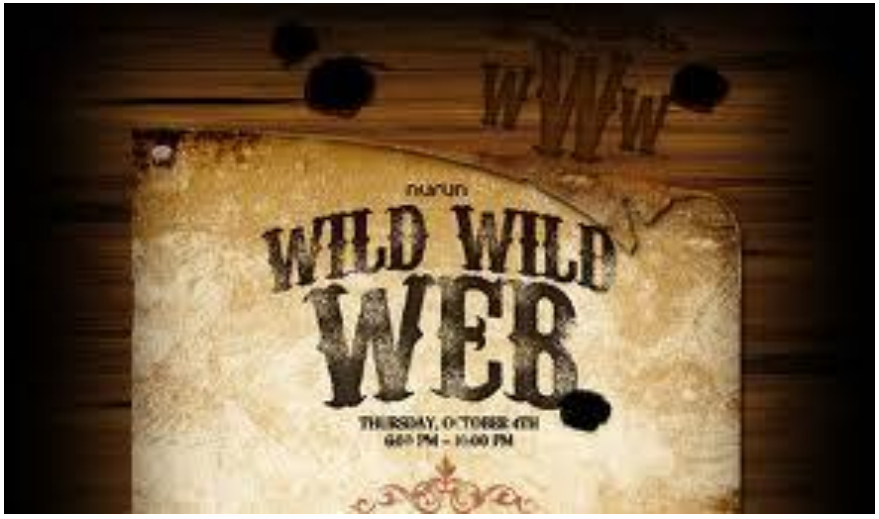
Defence in Depth

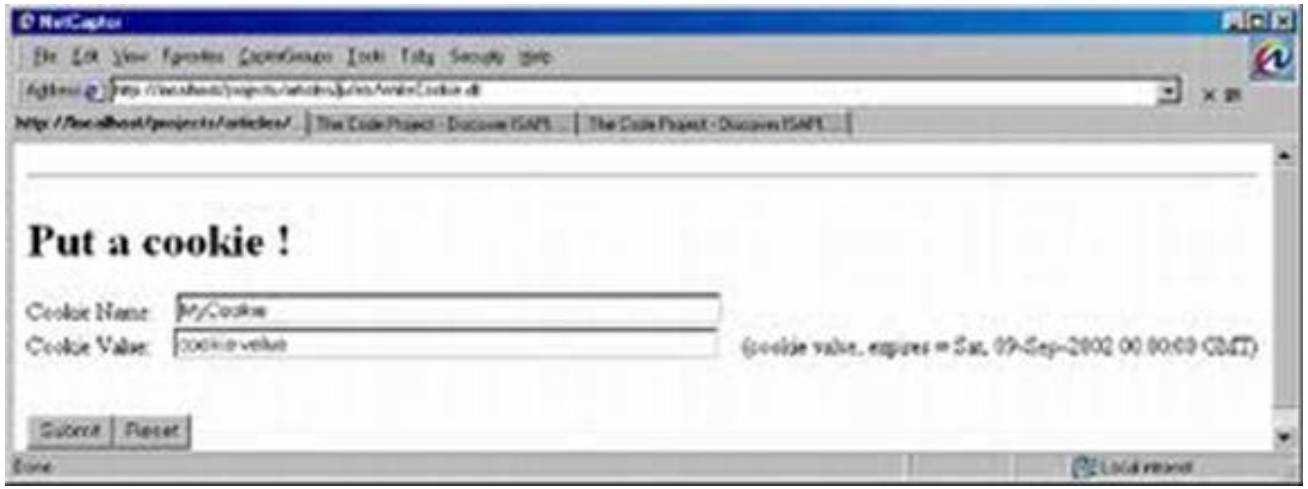


System of Controls



Information Security Concerns



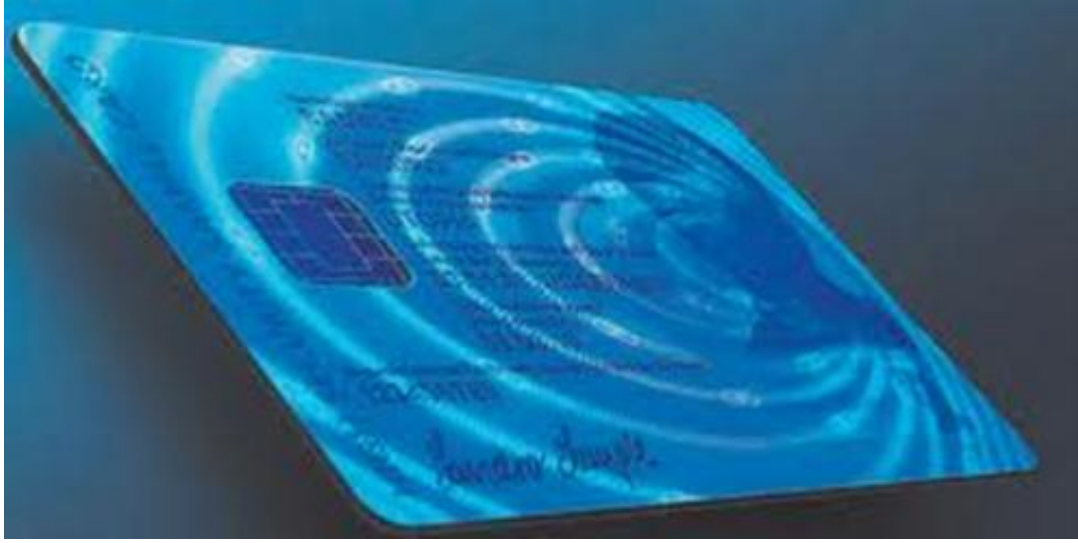

Put a cookie !
Cookie Name:
Cookie Value:
Submit
Reset


files
Trojan
target
computer
access
malware
horse
hacker
horses
perform
system
operations

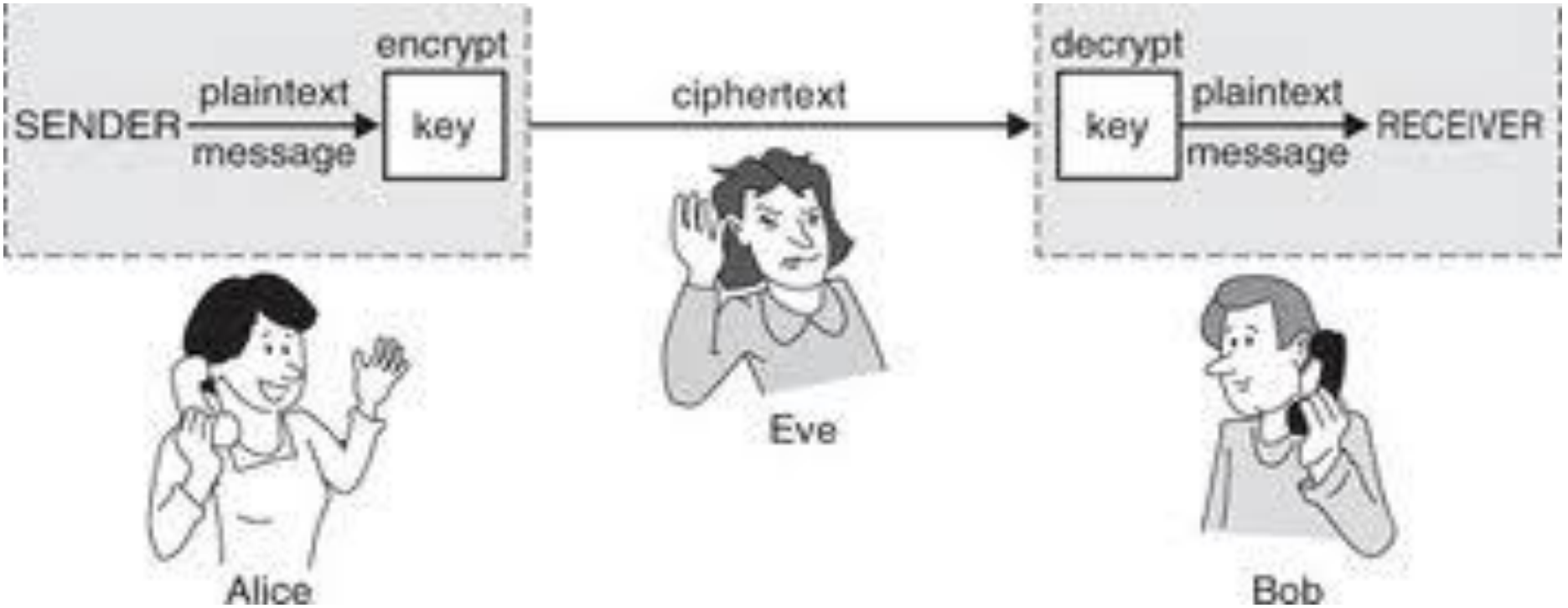

Steganography

All Threats: Attacks & Hazards! (video clip)

Future…



- Reduced Control
- More Complexity
- Cyber Warfare and Critical Infrastructure Attacks
- Increase Importance of Business Continuity
- Digital Identities and Wallets
- Increased Focus on Identity Management
- More Cloud and Mobile Computing
- Increased Use of Cryptography
- More Internet and IPv6


encrypt
plaintext
SENDER
message
key
ciphertext
decrypt
key
plaintext
message
RECEIVER
Eve
Alice
Bob

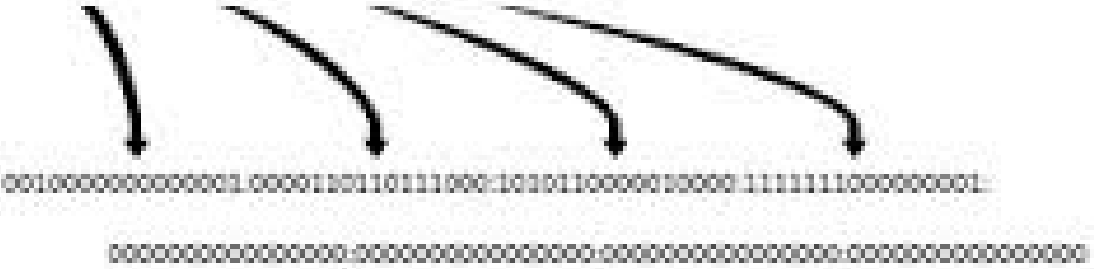

ATTACK
TOMORROW

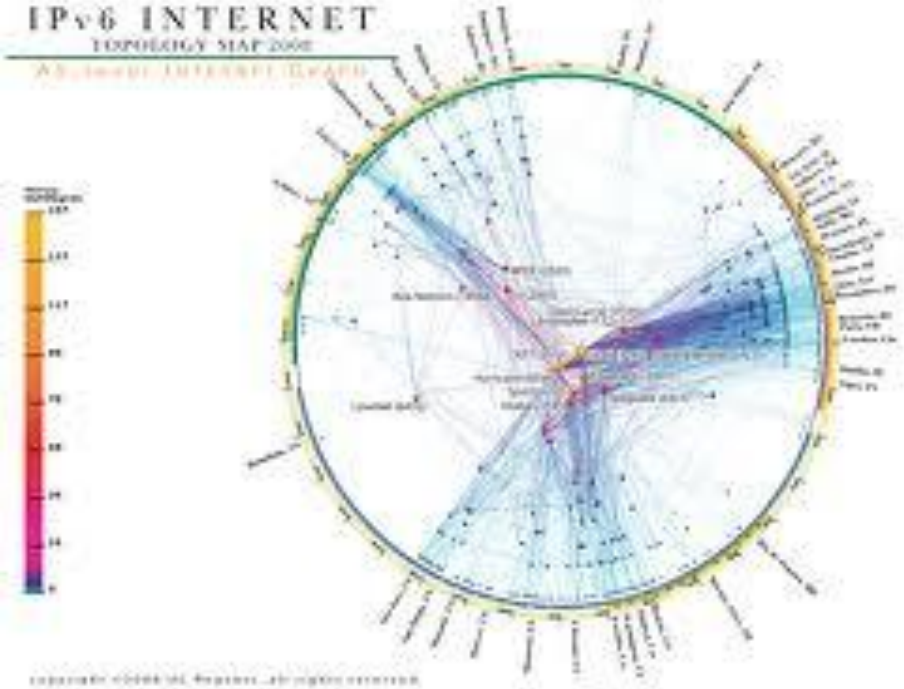
An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

2001:0DB8:AC10:FE01::

Zeroes can be omitted



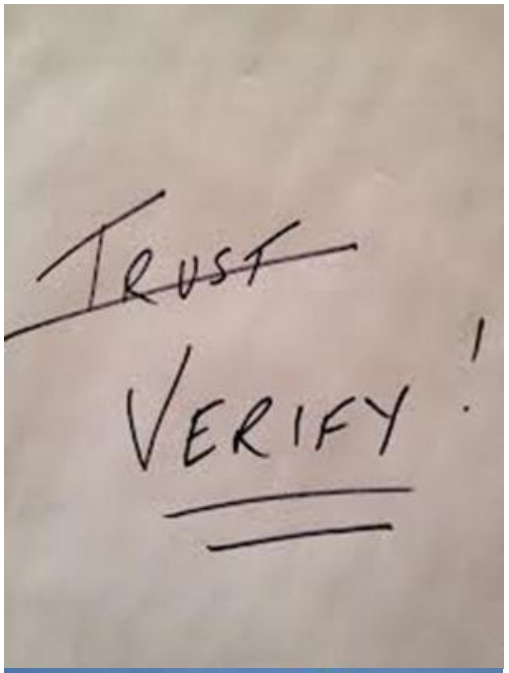


“There’s nothing remarkable about it. All one has to do is hit the right keys at the right time and the instrument plays itself.”

- Johann Sebastian Bach, (composer, 1685-1750)

Conclusion

- The Information Age has dawned!
- There is a Dark Side of Trust even in this new age!
- Information Security Must become a way of life for all!



University of Fort Hare

Together in Excellence

Abstract: Prof Stephen Flowerday
INFORMATION SECURITY AND THE DARK SIDE OF TRUST!

In her address to Parliament in 1586, Queen Elizabeth 1st (the British monarch) concluded with the words: "In trust I have found treason." With this statement in mind, the question to be asked here is at what stage is one relying on trust to the point that one is overly exposed to risk? In this regard, risk and trust are two sides of the same coin.

Information has become the world's most valued asset and we are well into the Information Age. Whilst we have embraced this new age, we have simultaneously exposed ourselves to new threats that exploit our vulnerabilities. While we enthusiastically adopt our connected lifestyles, including new technologies and optimised business processes, we expose ourselves to the villainous behaviour of intentional cyber attacks. The countermeasures and protection against such behaviour lag behind the drive for integrated information systems (including social systems) and the digital networked society, not to mention the unintentional information security errors or catastrophic events that may cause massive organisational failure when systems fail or irritation when data is lost or corrupted.

Nowadays, information security has become one of the most important topics for boards of companies, especially CIOs, governments and the general public, yet all security (be it military, physical or information) is viewed in terms of a cost and does not add directly to the bottom line; thus, security measures are habitually inadequate and this leaves individuals and organisations vulnerable. Consequently, as a result of the "cost" of information security, we justify increased trust levels which expose us to undue risk or the dark side of trust!

With the internet and its connected information systems being open systems, it becomes difficult to "control" the environment; hence, predictability is problematic and uncertainty high. In this environment we have organisations harvesting and storing large amounts of our personal data in huge server farms, with or without our consent. This is in addition to the cyber criminals, who are growing in number and sophistication in their attacks on our personal and corporate data.

As security is an all-or-nothing proposition, one needs to take a holistic view of it to ensure that all aspects have been attended to. The emergent properties of this holistic view should include increased predictability and reduced uncertainty; reflecting trust at an appropriate level that mirrors the risk appetite level. Furthermore, to develop trust in IT and information systems as a whole, a process should be followed which successfully identifies, assesses and controls risk. Only then can reasonable assurances be attained. Bearing in mind that information systems involve people, processes and technology, as well as principles of both art and science, the reductionist Newtonian mechanical view has been proven to be incomplete, even though popular with many computer scientists. This leads to systems theory, which is akin to holism and general systems theory, in terms of which one needs to focus on the sum of the parts and their relationships in order to ensure that the whole is achieved. Nothing should be done in isolation, in the hope that a deterministic approach will be sufficient and that no unpredictable consequences will follow.
My research focuses on the following issues: How does one ensure that information is kept confidential, yet is available to the right people at the right time, and that the information has integrity? These are the pillars of information security and if one addresses all three pillars, by applying a system of controls, ensuring defence-in-depth because risk is ubiquitous in nature, then reasonable assurance is likely.

University of Fort Hare

Together in Excellence

Stephen Flowerday - biography

Stephen Flowerday was born in Durban and grew up in Mount Edgecombe, later attending school at Cambridge in East London. He holds a BSc and an MBA, and obtained a DTech (IT) from the Nelson Mandela Metropolitan University (NMMU) in 2006. His thesis, "Restoring Trust by Verifying Information Integrity through Continuous Auditing", focused on a real-time system of controls for identifying accounting anomalies. He has published five refereed papers from this thesis.

He started studying for a BCompt degree while working as an article clerk in East London. He then changed to studying for a science degree and subsequently left the auditing profession. He spent the next twelve years studying and working as a management consultant both in South Africa and the United Kingdom. Midway through the year 2000 he returned to South Africa and entered academia as a senior lecturer in Business Information Systems at NMMU. Stephen has been in the Department of Information Systems at the University of Fort Hare since mid 2006.

In the last nine years, Stephen has authored and co-authored 41 refereed publications and has presented papers in various countries including China, Sweden, the United States of America, Kenya, Uganda, South Africa and the United Kingdom. He has worked on research projects with the CSIR, IBM and SAP AG and this has allowed him to collaborate with world-class researchers through his visits to their research laboratories in Pretoria, Israel and India. Furthermore, he acts as a reviewer for conference publications and academic journals and serves on various panels of the NRF. He has also been appointed as an external examiner for a number of universities, including Stellenbosch, Rhodes, Witwatersrand, NMMU, Johannesburg, Pretoria, UKZN, Royal Holloway (UK) and Karlstad (Sweden). In addition, he is an NRF-rated researcher (C3) and has supervised 26 postgraduate students to completion and is currently supervising eight Master's and Doctoral students in the field of trust, risk and information security.