CYBERSECURITY FOR CRITICAL INFRASTRUCTURE – LEGISLATION AND REGULATION
C Pool - Proconics

Engineering, Procurement, Construction, Project Management, Automation, Control, Electrical, Instrumentation, Design, Software Systems Integration and Analysers.

Agile, Interdepedent, Insightful, Relational.

LEADING THE ELECTRICITY DISTRIBUTION INDUSTRY

AMEU

Association of Municipal Electricity Utilities (Southern Africa)
Est 1915
AMEU

Proconics

Contents

- Who am I?
- Introduction
- Legislative
  - History
  - Cybercrimes & cybersecurity bill – 2017
  - OHSACT
- Standards
- Conclusion
- Questions

Who am I?

- 22 years in industry
- 14 years involved in process networks & security
- ECSA Pr. Eng

Certificate of Training

Presented by the

Industrial Control Systems Cyber Emergency Response Team
U.S. Department of Homeland Security

To

Cobus Pool

For completion of the following course:

210W - Cybersecurity for Industrial Control Systems

April 25, 2014

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
National Cybersecurity and Communications Integration Center (NCCIC)
U.S. Department of Homeland Security

Introduction

- Cybercrime reported impact 2015 – R35billion
- 3rd most active country for cybercrime
- Industrial systems including smart grids at risk
- Aurora – grid specific
- General malware

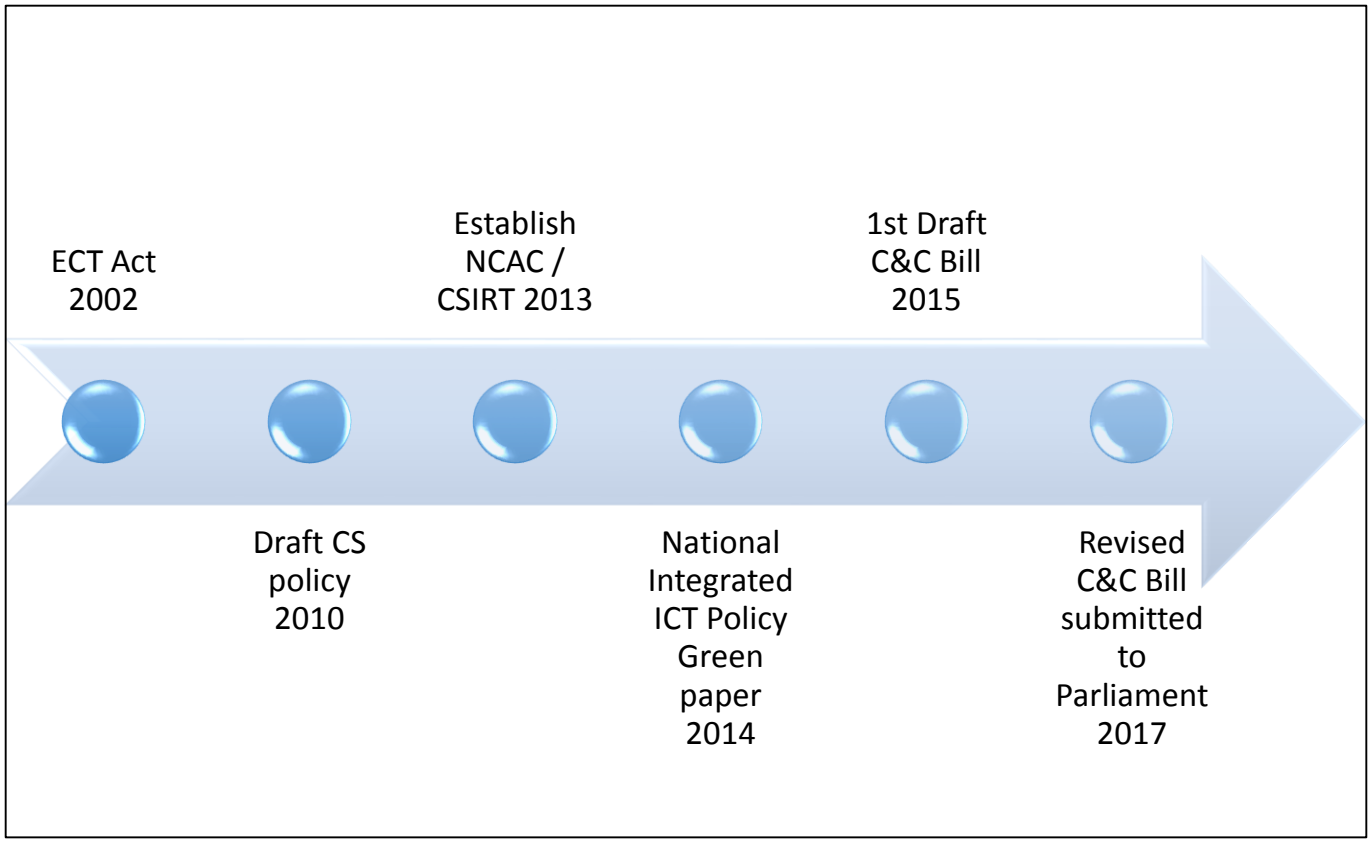
Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	1. Malware	↑	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Denial of service	↑	↑
5. Denial of service	↑	5. Botnets	↑	↓
6. Physical damage/theft/loss	⊃	6. Phishing	⊃	↑
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	↑
8. Phishing	⊃	8. Ransomware	⊃	↑
9. Spam	↓	9. Insider threat (malicious, accidental)	⊃	↓
10. Exploit kits	↑	10. Physical manipulation/damage/ theft/loss	↑	↓
11. Data breaches	⊃	11. Exploit kits	↑	↓
12. Identity theft	⊃	12. Data breaches	↑	↓
13. Information leakage	↑	13. Identity theft	↓	↓
14. Ransomware	↑	14. Information leakage	↑	↓
15. Cyber espionage	↑	15. Cyber espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

LEADING THE ELECTRICITY DISTRIBUTION INDUSTRY

Proconics

Legislation - History



Legislation – C&C bill

- Chapter 2 – definition of crime:
  - Unauthorised access
  - Interference with data & essential services
  - Failure to comply can result in 2 year sentence
- All NKP's are automatically included
- Responsibility of owner / operator of critical information infrastructure
  - Apply to have the infrastructure declared critical
  - Comply with directives (at own cost)
  - Audits to be performed every 24 months (Section 58)
- Security to be maintained according to national standards
- SSA – concerns expressed

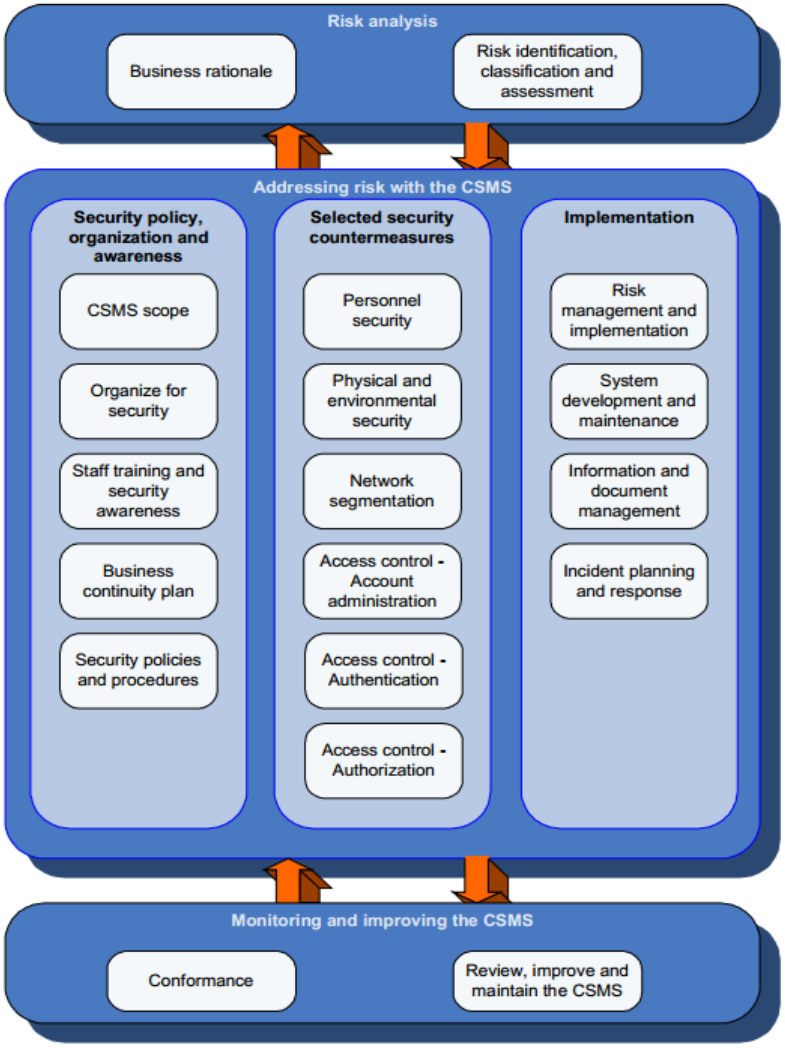
Legislation – OHSACT

- Controversial
- GMR 3 & 4
  - ICS's can be fined as part of machine assemblies
  - Securing & safe operation regulations apply
- MHI Regulation 6 (Generally not applicable to Electricity distribution)
  - Risk assessments
  - Audits
  - Mitigation of risk

Standards – SANS62443-2-1

- SATS62443-1-1 also accepted
- Only part of IEC62443 suite
- CSMS
  - Risk analysis
  - Addressing the risks
  - Monitor and improve the CSMS
- Dependant on 2 principles
  - Defence in Depth (DiD) – this includes isolation of functional and logical units
  - Continuous monitoring and improvement.

Standards – SANS62443-2-1

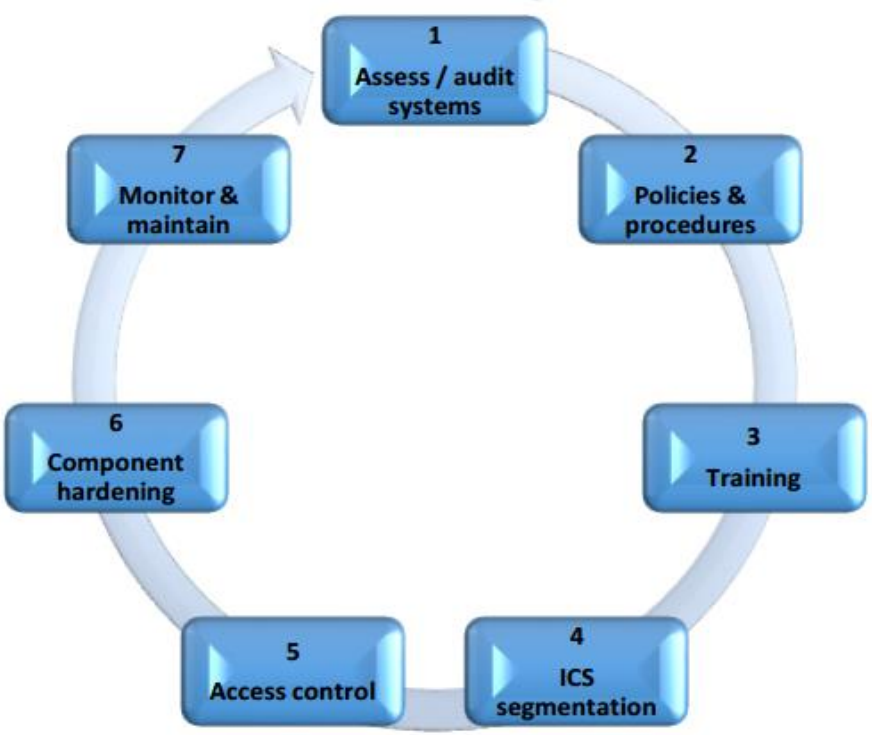


Standards – SATR62443-3-1:2016

- Implementation technologies
  - Authentication & authorization – includes password management
  - Filtering / blocking / access control – does not include physical access control, but includes firewalling
  - Encryption & data validation – includes VPN's
  - Management, audit, measurement, monitoring & detection – includes antivirus, IDS and automated software management
  - IACS software – covers the different operating systems
  - Physical security – access control and personnel security

Standards – SATR62443-3-1:2016

- Industry specific guidelines should be used
  - NERC CIP, NIST, ENISA



Conclusion

- ICS systems at risk
- Legislative impact
- Be proactive

Questions?