A Maturity Model for National Cyber Security Strategy

Almerindo Graziano, PhD
Silensec

ITU-ATU Workshop on Cybersecurity Strategy
in African Countries
Khartoum , July 2016

silensec
Information Security Since 1998

About Silensec

- Information Security Management Consultancy Company (ISO27001 Certified)
  - IT Governance, Security Audits
  - Security System Integration (SIEM, LM, WAFs)
  - Managed Security Services
- Offices: England, Cyprus, Kenya,
- Cyber Threat Intelligence
  - Monitoring, Threat Assessment, Investigations
- Independent Security Training Provider
  - ISO27001, Business Continuity, PCI DSS, CISSP, Ethical hacking, Computer Forensics, Mobile Forensics, Reverse Engineering, Intrusion Detection, Log Management

Cyber Threats Scenario Today

Threat Actor	Description and Motivation	Potential Targets	Goal
Cyber Criminal	Varying degree of competence. Usually motivated by the achievement of financial gain or the affirmation of private justice	Potentially any target for personal reasons or as “for-hire guns” by a third party threat actor	Financial gain, private justice
Organized Crime	Structured, funded, consisting of different roles with associated competences and responsibilities. Usually motivated by the achievement of financial gain. Can be hired by other threat actors (e.g. industrial espionage, internal threats etc.)	Commercial organization but potentially any target as “for-hire guns” by a third party threat actor	Financial gain
Hactivists	Typically decentralized groups or individuals with varying degree of technical skills. Highly motivated by their ethics and principles and the advancement of a cause	Targets are specific to the sectors of interest to the activist group (environmentalist, animal lovers etc.)	To cause reputational damage or advance specific causes through information gathering
State-sponsored criminals	Technically skilled with virtually unlimited resources at their disposal, motivated by the country political agenda	Foreign government institutions and officials, large foreign commercial organizations	Acquire information, monitor and control
Competitors/ Industrial Espionage	Good level of resources and varying degree of comptences, usually motivated by the achievement of business objectives	Targets varies according to the relevance to the threat actor	Acquire information, disrupt business (image, reputation and operations)
Employees/Internal Threat	Quite varied in age, techinal competence and intent but all in possession of sensitive information that has a critical impact to the organization. Can be used by other threat actors. Motivated by malcontent, spirit of revenge or financial gain	Typically commercial organizations but potentailly applicable to any type of organization	Personal gain or revenge
Opportunists	Unaffiliated hackers (usually young) looking for recognition by the hackers community and for new learning opportunities. Rarely financially motivated	Various targets both from the private and public sectors. Target sensitivy varies with the capability of the threat actor.	Achieve recognition, improve competence

National Cyber Security Startegy

- A National Cybersecurity Strategy is the expression of the vision, high-level objectives, guiding policy principles and explicit accepted priorities that a country adopts to address specific cybersecurity issues.

Benefit of a NCSS

- The aim of a cyber security strategy is to increase the global resilience and security of national ICT assets, which support critical functions of the state or of the society as a whole.

NCSS Strategic Areas

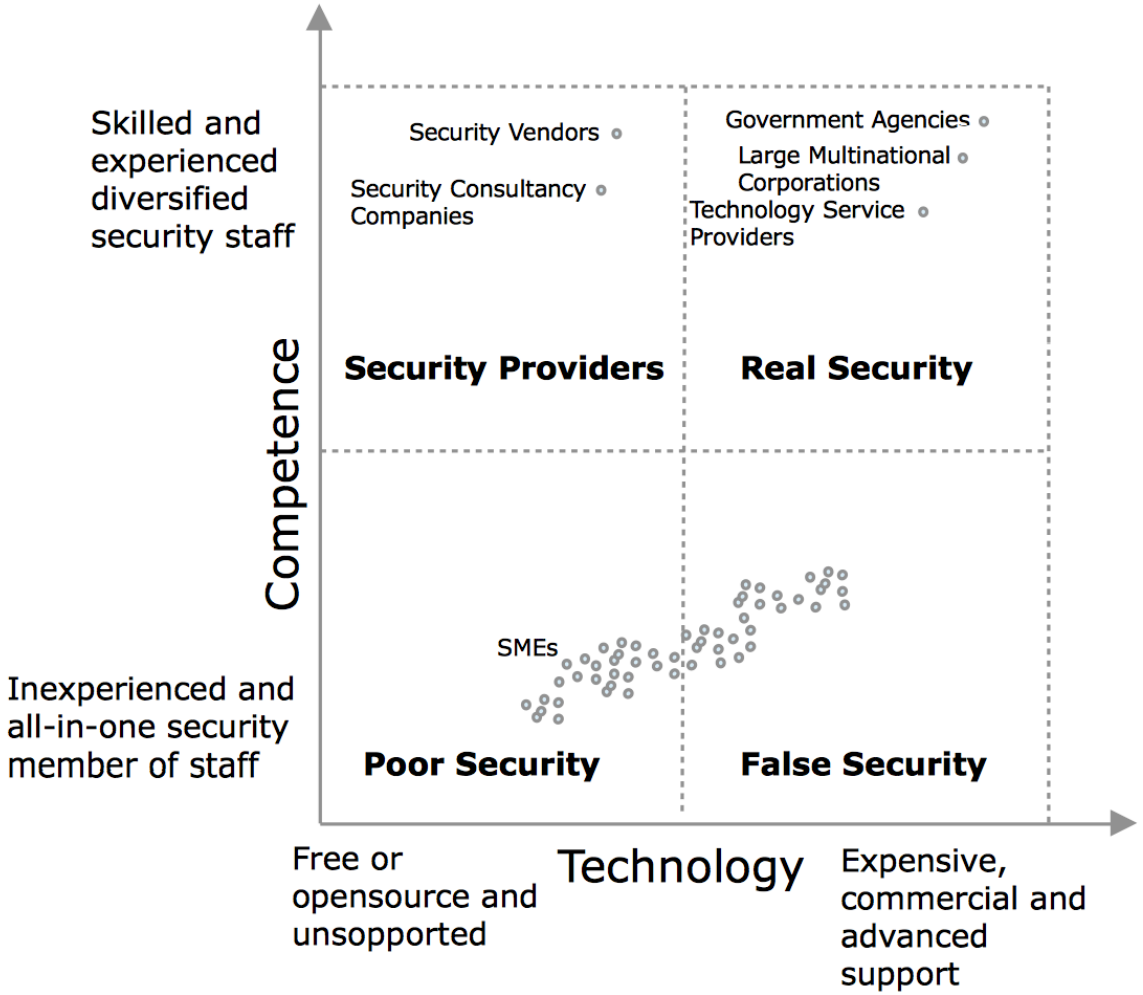
#	STRATEGIC AREA	DESCRIPTION
1	GOVERNANCE	This strategic area introduces the steering of the NCS, framework and implementation plan, outlining organizational and positional authority (determination of responsibilities) within the government and of multi-stakeholder cooperation mechanisms. It also includes allocation of human and financial resources, and NCS review cycle.
2	RISK-MANAGED RESILIENCE	With this strategic area governments can focus on the development of regulations, standards, and policies that form the national cybersecurity framework.
3	PREPAREDNESS AND INCIDENT RESPONSE	This strategic area looks at detection of, response to and management of cyber incidents of national interest in a coherent manner with continuous improvement of response capabilities and coordination.
4	CRITICAL INFRASTRUCTURE	Through this strategic area, creation of concepts to identify and protect information digital assets and infrastructures, including critical services (e.g. energy, finance, water, transports, telecommunications, etc.), are introduced.
5	CAPABILITY DEVELOPMENT AND AWARENESS	Within this strategic area the advancement of national cybersecurity capabilities through research and development (R&D) programs is encouraged. Moreover, this area includes the development of programs to foster cybersecurity awareness, education and skills development and the development of a specialized workforce.
6	CRIMINAL JUSTICE	This strategic area prioritizes the formalization of a legal framework defining illegal cyber activities and establishing the agencies that will enforce the legal framework (e.g. police, prosecutors, judges).
7	INTERNATIONAL COLLABORATION	This strategic area seeks to encourage outreach, partnership, and information sharing activities among nations and governments, and allow governments agencies to leverage existing capabilities and knowledge.

Source: ITU

About Africa Cyber Security Research

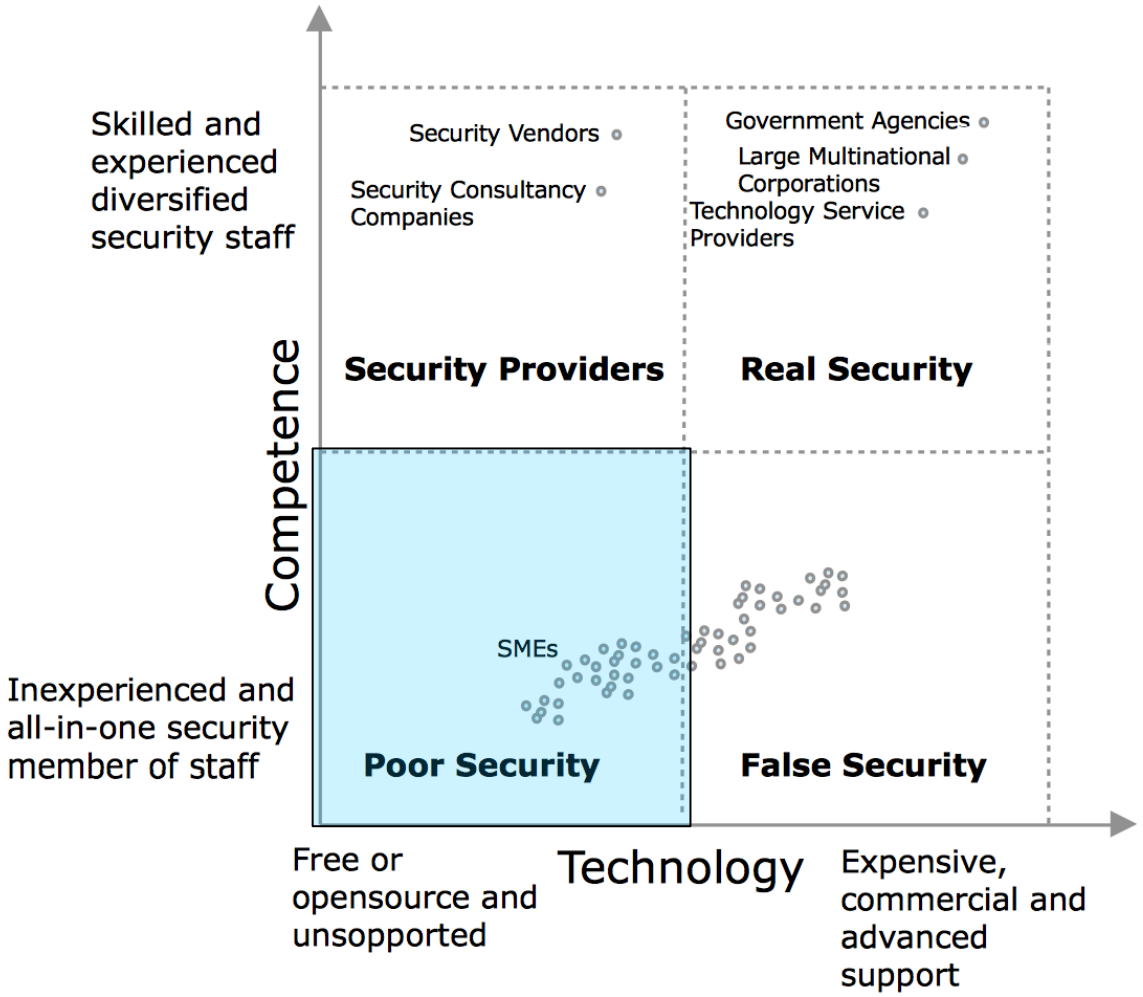
- Over 500 organizations across Africa
- Three main sectors
  - Banking/Financial
  - Telecommunication
  - Government
- Work in progress conducted by Silensec research related to Information Security Maturity models

Silensec Security Quadrant



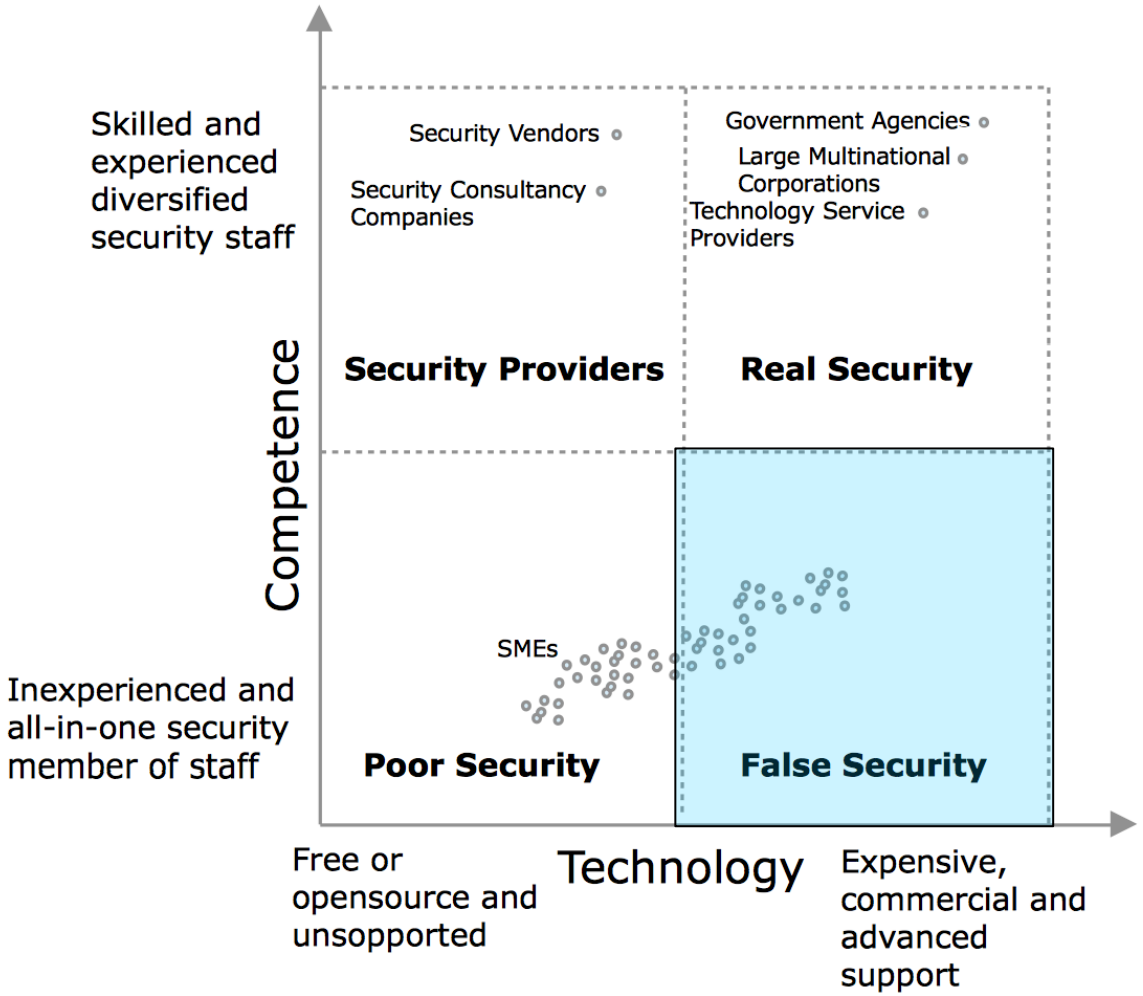
- Competence
  - Staff competence
  - Defined roles and responsibility
  - Management of Information Security
- Technology
  - Tools and systems and technologies to provide security controls

Silensec Security Quadrant – Poor Security



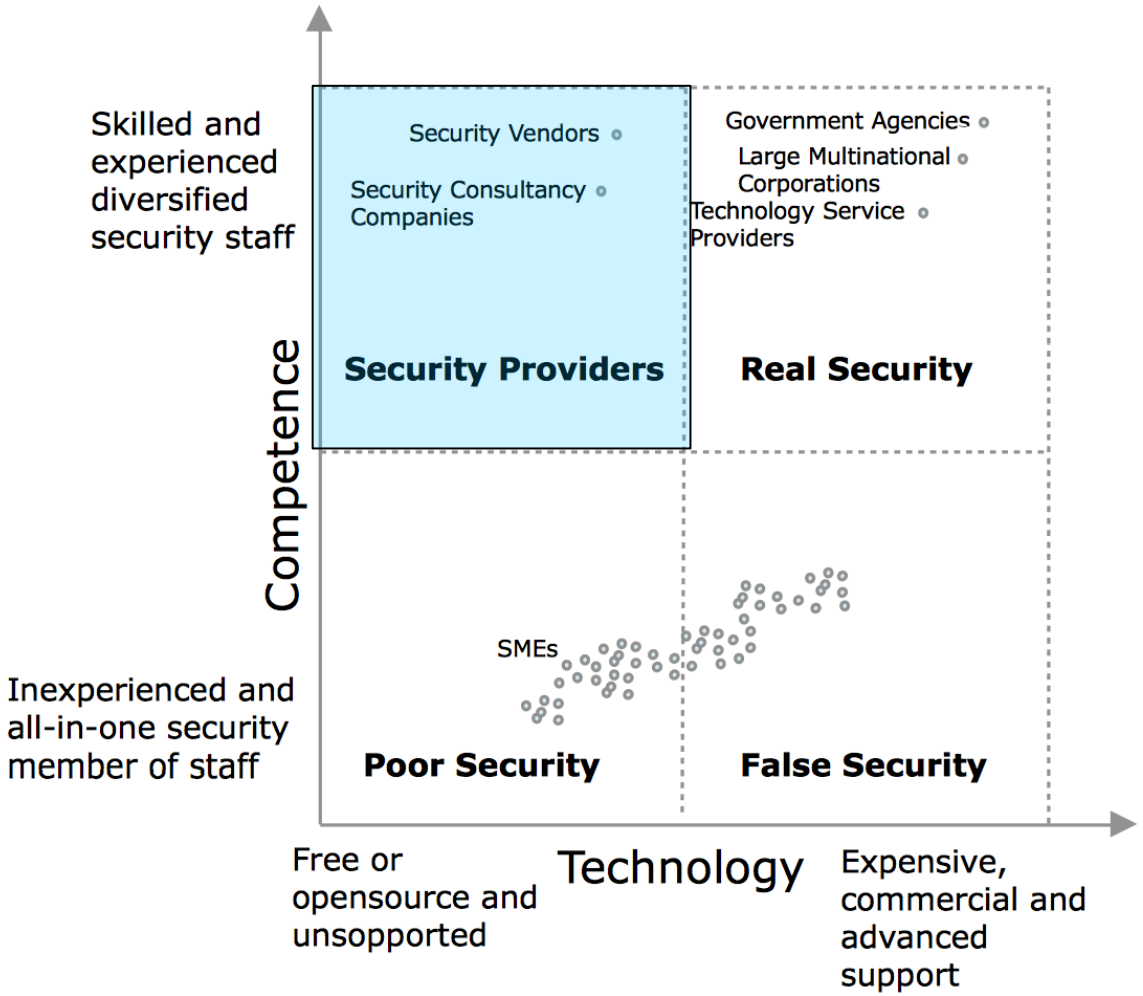
- **Competence**
  - Weak Staff competence
  - Roles and responsibilities not clearly defined
  - No formal management of Information Security
- **Technology**
  - Little or no security technology
  - Mostly open source with some commercial tools

Silensec Security Quadrant – False Security



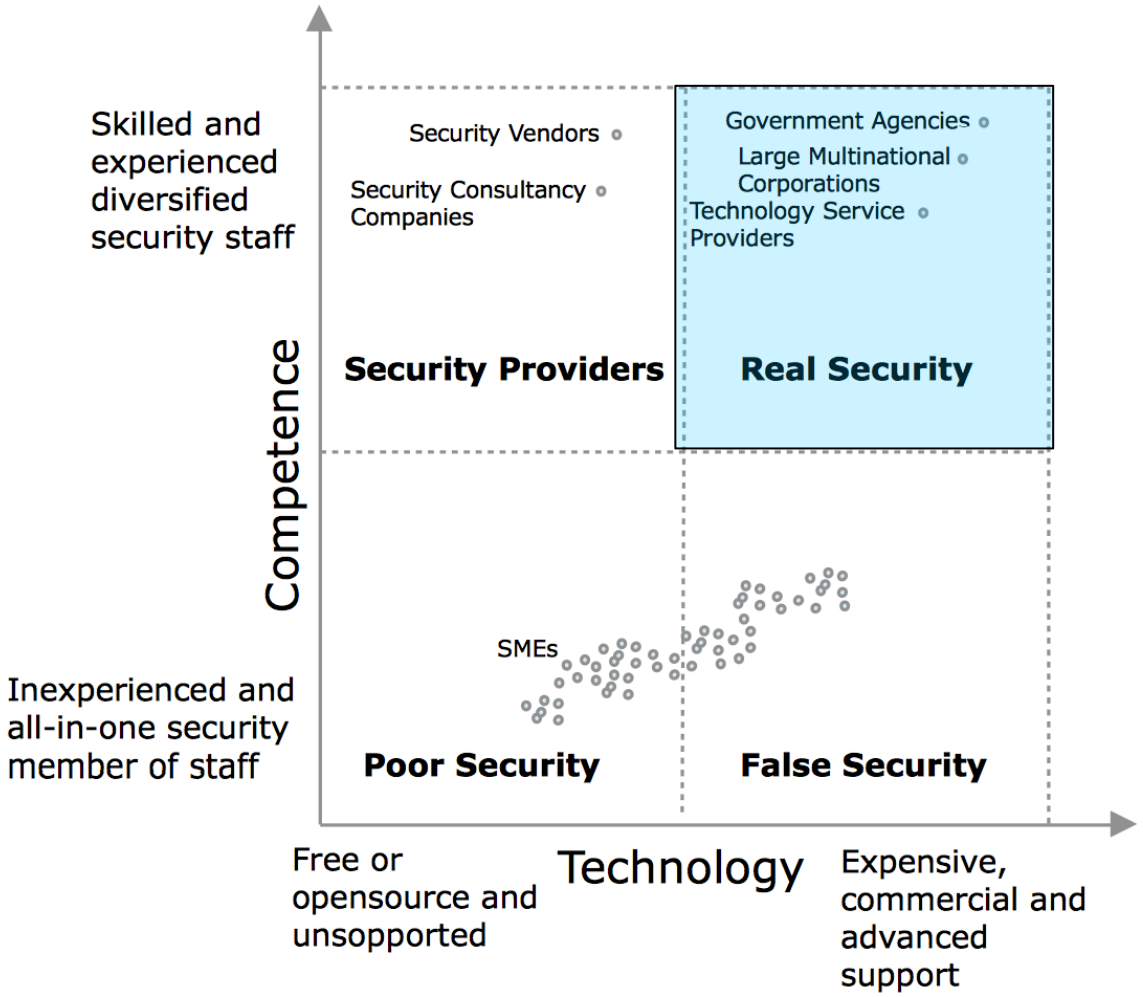
- Competence
  - Some level of staff competence
  - Some roles and responsibilities
  - Some (often formal) Management of Information Security
- Technology
  - More investment in security tools and technologies
  - Over reliance on technology

Silensec Security Quadrant – Security Providers



- **Competence**
  - High level of staff competence
  - Clear roles and responsibility
  - Strong management of Information Security
- **Technology**
  - Strong use of "free" technology
  - Use of commercial tools to the extent needed

Silensec Security Quadrant – Real Security

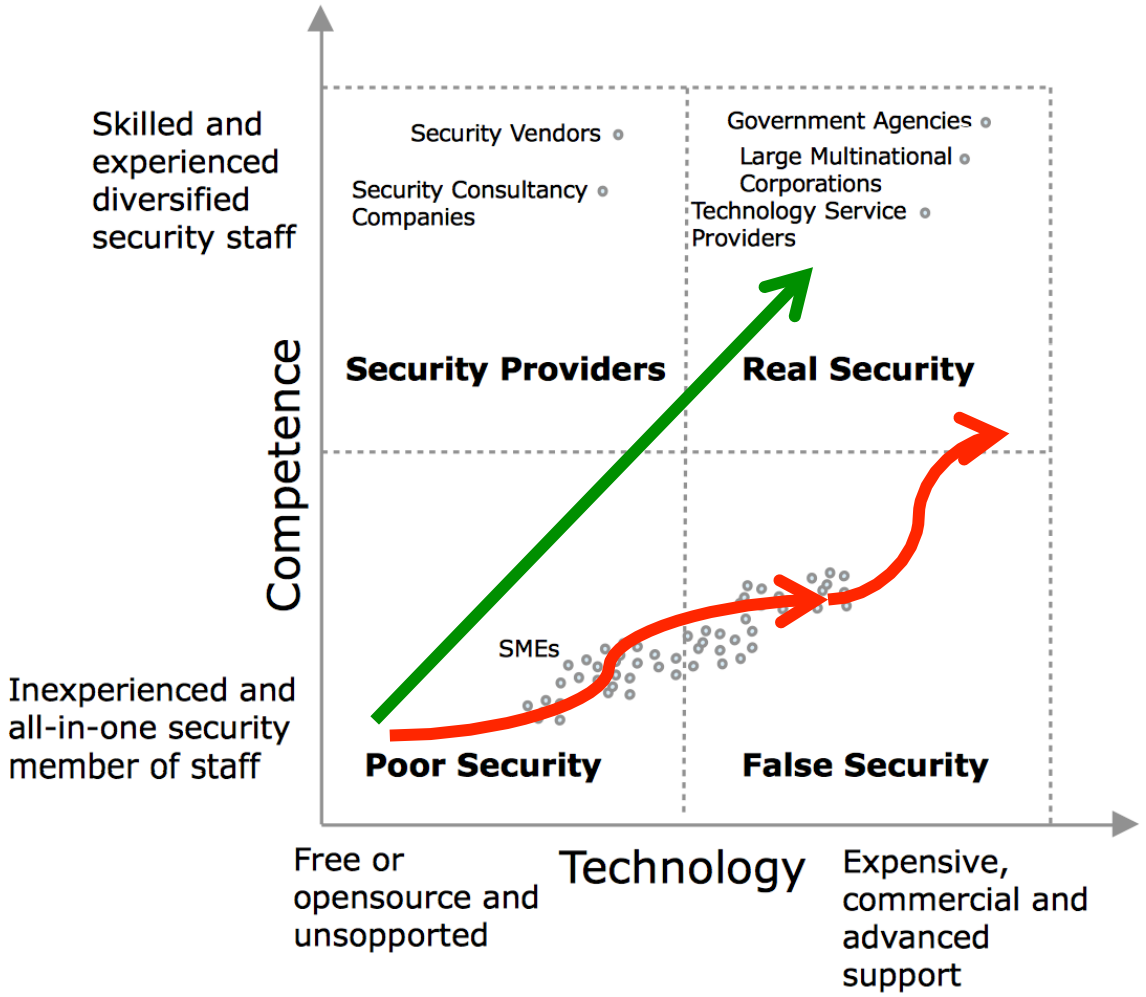


- Competence
  - High level of staff competence
  - Clear roles and responsibility
  - Strong management of Information Security
- Technology
  - Strong use of comemrcial security products and services
  - “free” technology

What is Maturity? – A Man Example

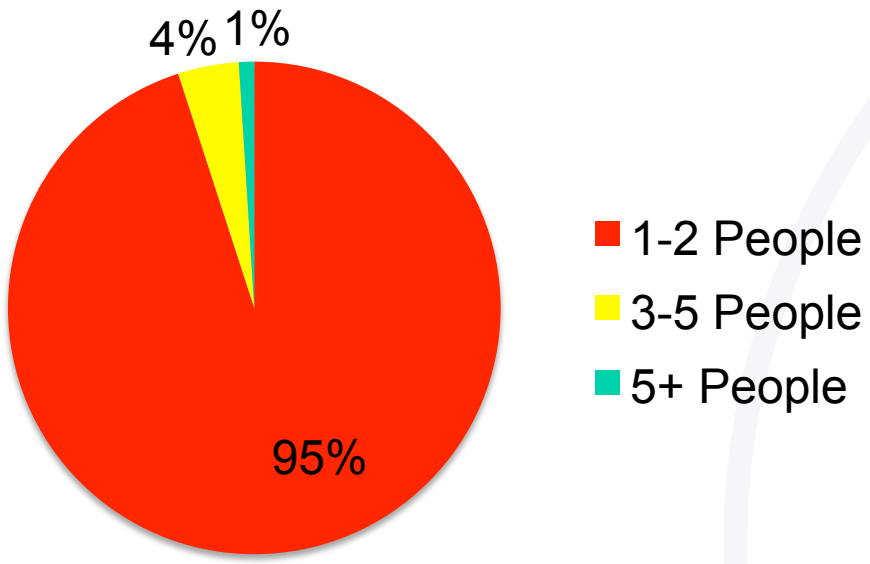
- Physical
- Mental
- Spiritual
- Social
- Family
- Professional

Adopting Security Maturity Model



Organization of information security

- Size of the security department



- No Information Security Role and very little decision power

Developing a Clear Governance Structure

- A governance framework defines the roles, responsibilities and accountability of all relevant stakeholders.
- It's implementation highly depend on the NCSS maturity level
- Sample areas of responsibility
  - Citizen Awareness & Cyber security Competence
  - Research and Development
  - International Cooperation
  - Public–Private Partnership
  - Fighting Cybercrime
  - Baseline security requirements
  - Incident response capability

Citizen Awareness and Competence

- Define Policy and Objectives
- Identify target audience
- Needs assessment
- Strategy

- Develop Learning Material
- Roll out programme

- Monitor Execution
- Review effectiveness

- Improve Programme
- Update material

Citizen Awareness and Competence

Building Competence

- Governance
  - Best practice standards, frameworks and guidelines
  - Risk Management
- Technical Competences
  - Prediction (Cyber Threat Intelligence)
  - Prevention (Security assessments and controls)
  - Detection (Security monitoring)
  - Reaction (Incident response and investigations)

Follow a national risk assessment approach

- Resources are finite and must be rationalized to prioritize cyber security risks
- Best practice approach when assessing the risks at national level is to follow a all-hazard approach
  - Incorporating all kinds of cyber threats such as cyber crime, hacktivism, technical failures or breakdowns)

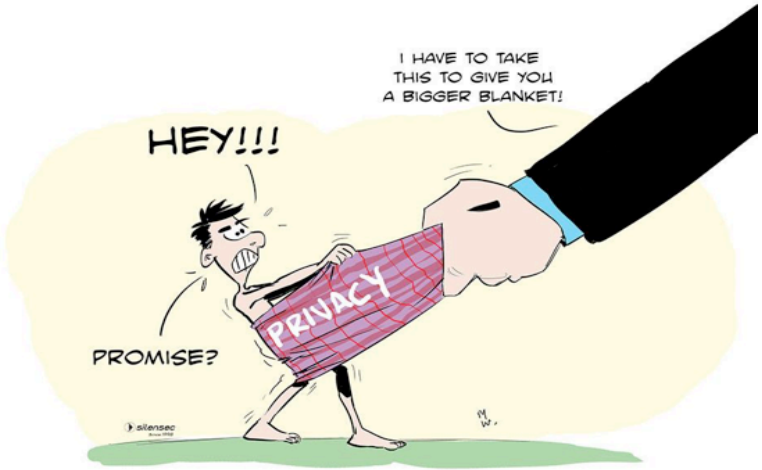
Follow a national risk assessment approach

Developing a Risk Assessment Methodology

- Any methodology can be used
- Risk Criteria
  - Impact Criteria
  - Evaluation Criteria
  - Acceptance Criteria

Silensec Cyber Security Awareness

- Free Awareness Cartoons
  - Security Awareness
  - Security Editorials
  - Life of the Security Consultant



Thank you
Questions?