www.pwc.com

"Human Firewalls"

Making your people a "cost" effective line of defence

IT Audit, Security and Governance Challenges in Financial Crisis" - December 2nd, 2011

pwc

PricewaterhouseCoopers S.A.
268 Kifissias Avenue
152 32 Athens, Greece
Telephone (+30) 210 68 74 714
Facsimile (+30) 210 68 74 444
stan.voulanas@gr.pwc.com

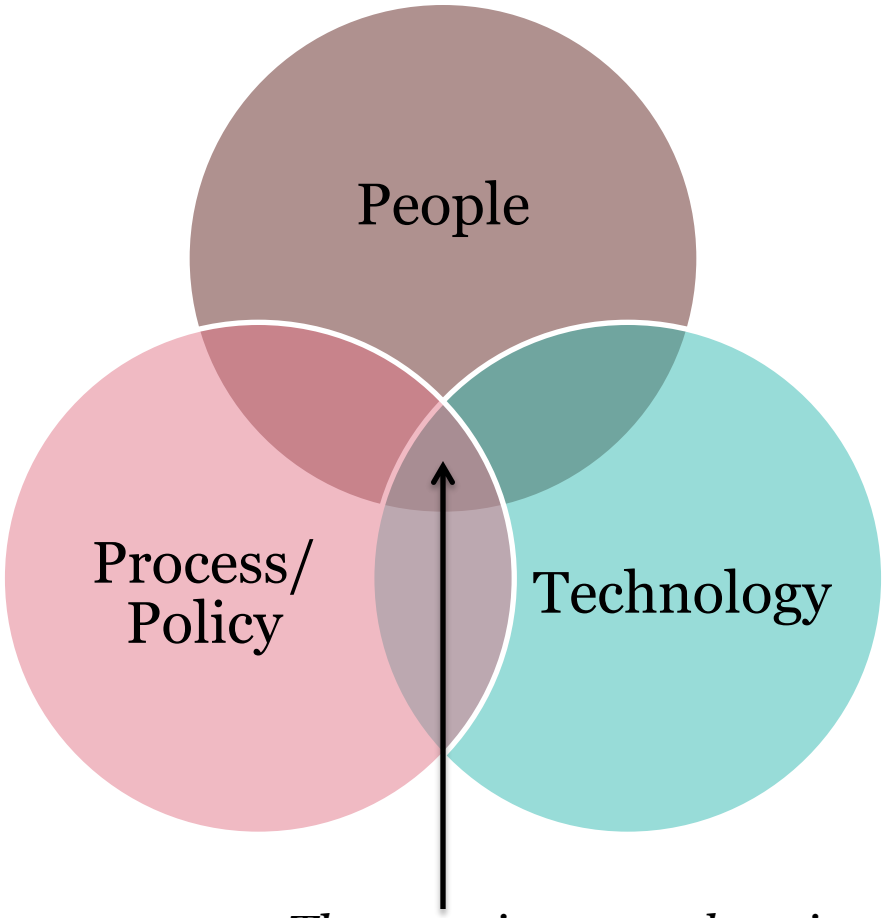
Asterios (Stan) Voulanas
Partner
Technology Risk Assurance

Agenda

- Introduction
- Key Drivers
- Approach & Methods
- In Summary
- Questions

Introduction

Security Positive Environment



People *— the people execute and support or comply with process, policy or technology*

Policy/Process *— supporting documentation and directions*

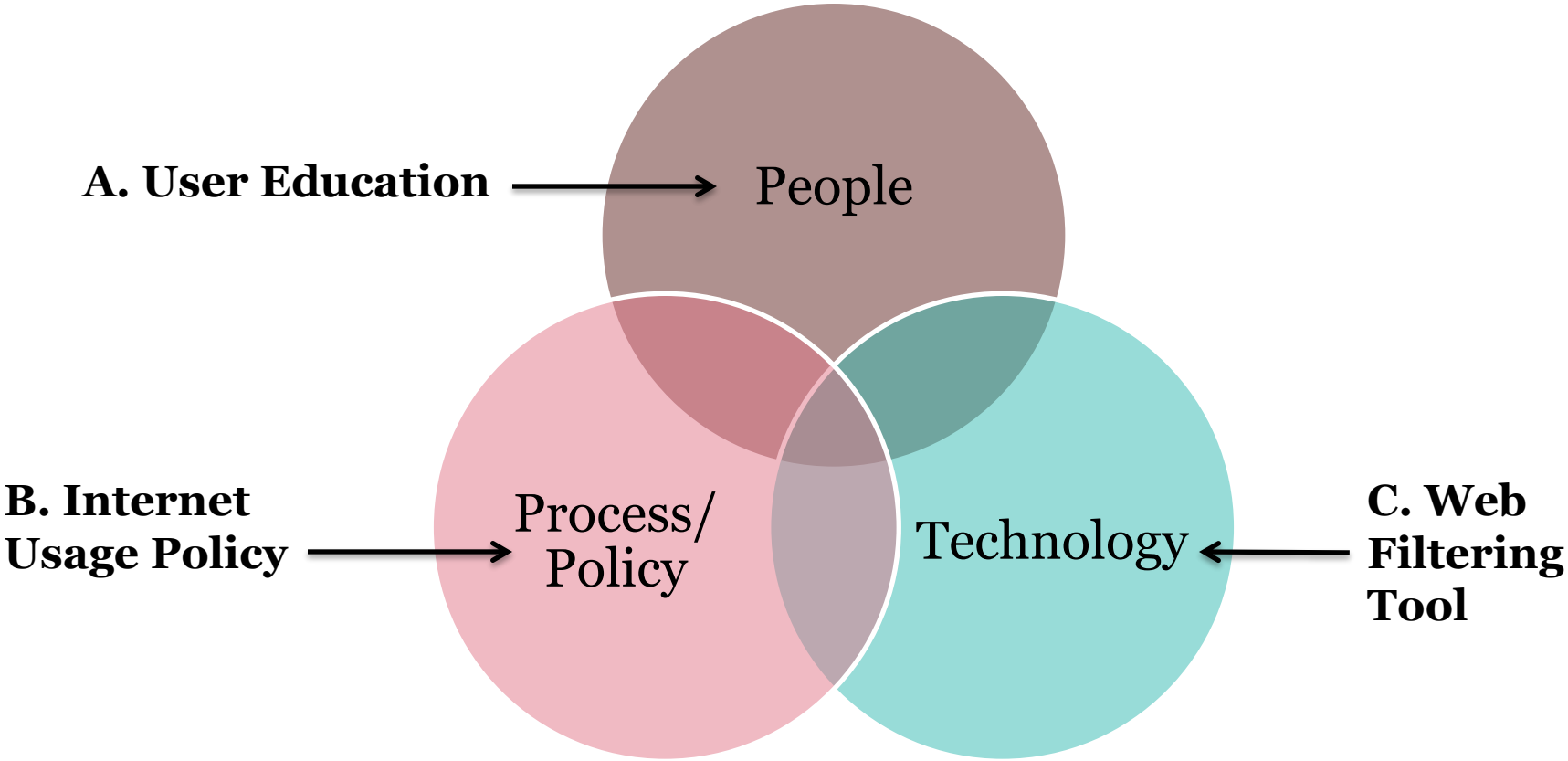
Technology *— the tools (H/W & S/W) facilitate the process or policy*

The security control environment is greatly enhanced when these three elements work in combination

Introduction

Security Positive Environment

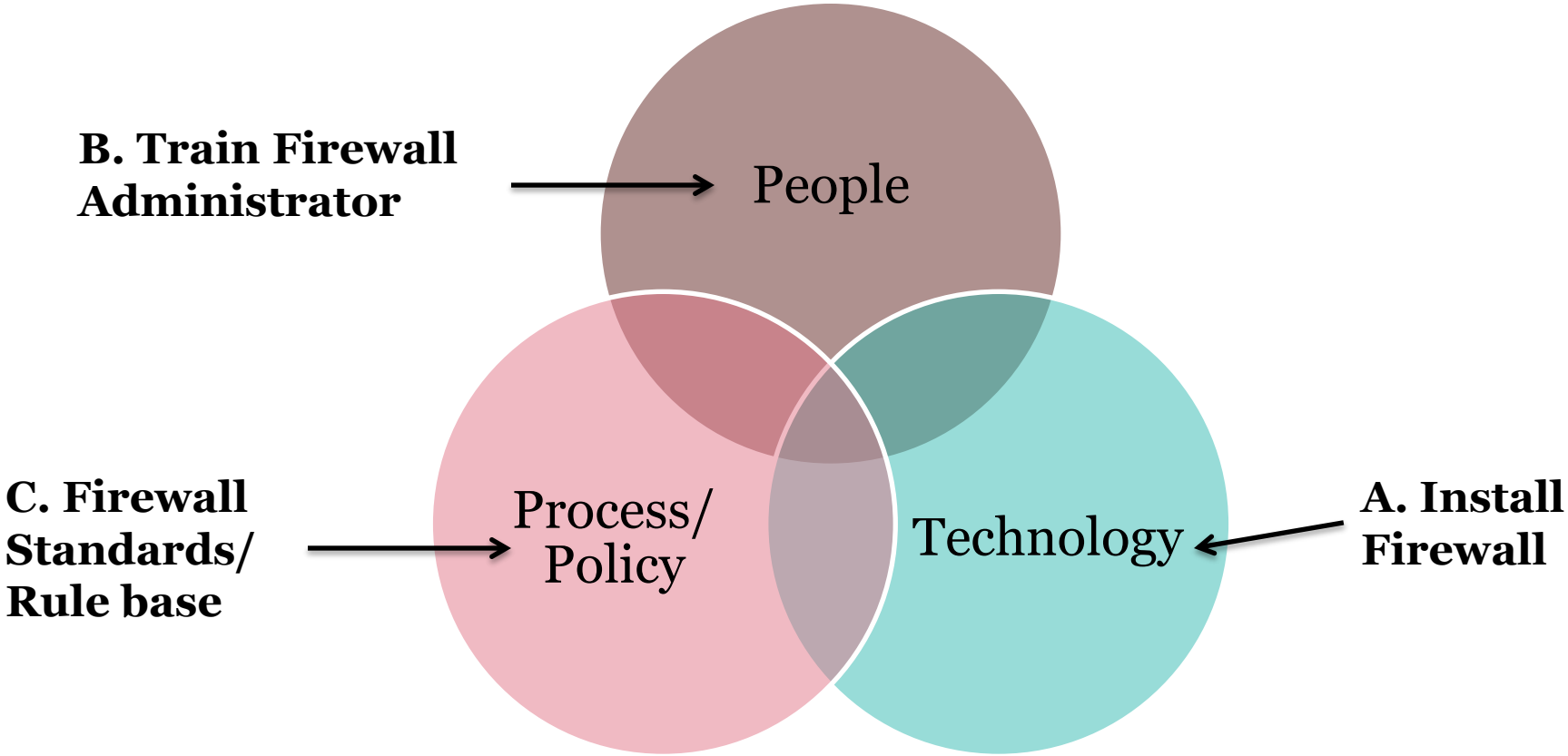
Internet Usage and Misuse



Introduction

Security Positive Environment

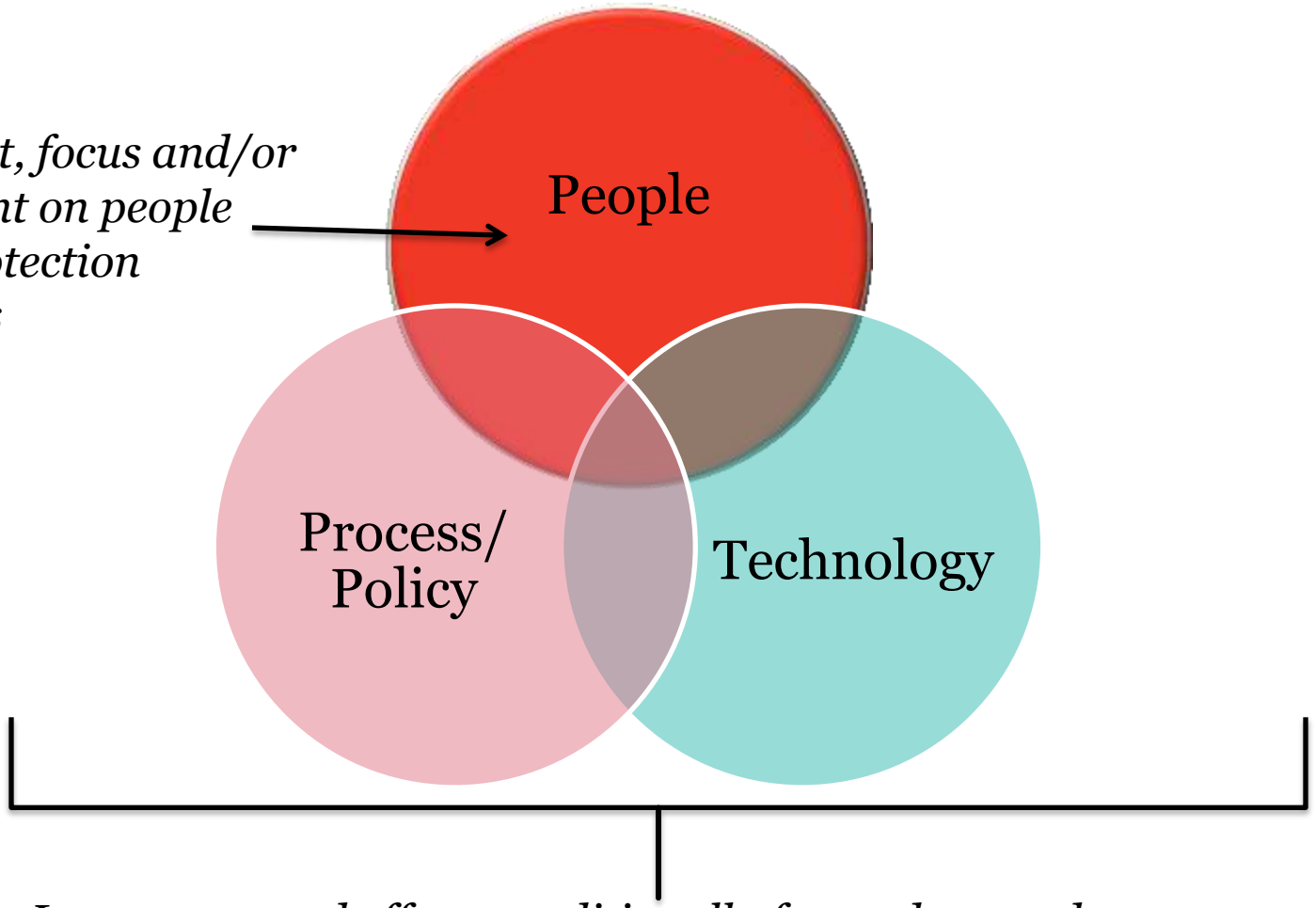
Firewall Policy



Introduction

Security Positive Environment

Less effort, focus and/or investment on people based protection strategies



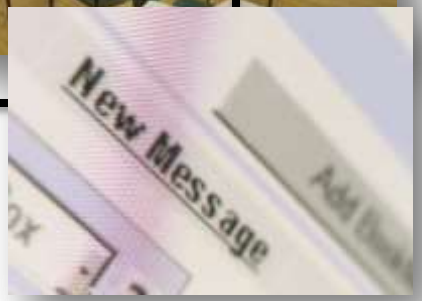
Investment and efforts traditionally focused towards technology or policy development based protection strategies

Introduction
Typical "People" Strategies

IT Security Organisation

IT Policies

IT Standards



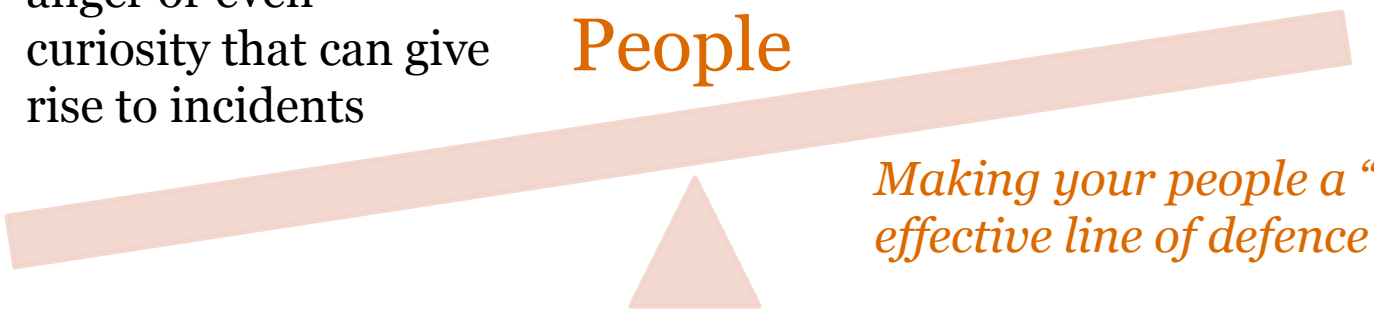
End Users of information & systems

Introduction

"People" based protection strategies

"Security aware" employees will often be best placed to identify a potential breach or a weak link and reduce the impacts of incidents when they do occur

There is always a human element ; negligence, ignorance, anger or even curiosity that can give rise to incidents



Making your people a "cost" effective line of defence

Getting the right balance

Introduction

"People" based protection strategies

Making your people a "cost" effective line of defence

So how do we achieve this ?

1. Understanding the key drivers and the changing trends around people security behaviours ("Soft" factors); and

2. Adopt a well planned approach using focused methods to change people's behaviour in a sustained manner

Key Drivers
Social networks

In today's socially connected workplace, employees swap updates on Facebook and Twitter, log opinions at blogs, and upload snapshots to photo-sharing sites..... a phenomenon that will only continue to gain force.

During the first half of 2009, 19 percent of all Internet attacks targeted social networking sites. This represented a dramatic increase over previous years, according to a study by Breach Security Inc.

- Employees may easily leak sensitive information via the use of social networks
- Social networks provide ambitious cybercriminals with as additional launching pads to exploit vulnerable corporate networks or users (end points)
- The user or workforce education is key to responsible use of social networks

Key Drivers

Mobile devices

The proliferation of mobile devices including portable storage devices are causing significant security challenges

- Portability – they tend to get lost /misplaced and tend not to be well protected
- Mobile storage devices are cheaper, increasing storage capacity and getting smaller
- Work provided mobile devices are also used by employees for personal activities
- Many employees tend to use their personal smartphones and other mobile devices to handle work-related tasks *(shadow IT)*
- Use of public (and insecure) wireless access points

…In April 2011, Google removed 55 apps from its Android Market after tens of thousands of users downloaded applications that were infected by the DroidDream trojan. The list of infected Android applications included Chess, Super Guitar Solo, Bowling Time, Super History Eraser, and Photo Editor….

- Users typically engage in high risk behavior – users sometimes keep passwords, pin codes or credit card details, download apps etc

Key Drivers
Complexity & Rapid Evolution

- Technology is evolving at a more rapid pace as are the related security threats - *zero day exploits, cybercriminals are beating the patch cycle*

- Sophistication of attacks (Attacks are much more targeted and sophisticated - *attackers are more patient harvesting information over long periods without detection e.g. APTs)*

- Complexities in technology demand better trained IT / and security staff

- New IT delivery models such as cloud computing require new security approaches

"The most recent threat landscape report from Forrester claims the gap between hacker threats and suitable security defenses is widening, at a faster pace than ever before" – "The New Threat Landscape: Proceed With Caution Understand The New Threat Paradigm To Make Your Responses More Effective by Khalid Kark (survey of 2,803 IT executives and technology decision-makers, August 13, 2010

Key Drivers
Regulation & Compliance

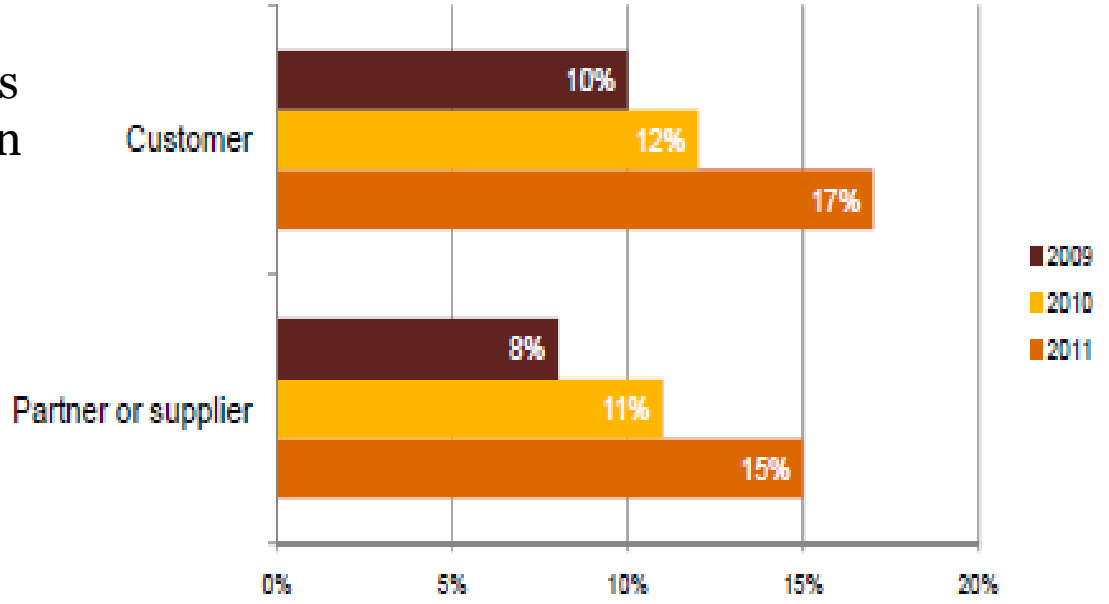
Standard	Reference in standard
ISF Standard of Good Practice for Information Security (2007)	SM2.4 Security awareness Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the organisation.
ISO/IEC 27002 (2005)	8.2.2 Information security awareness, education, and training All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant to their job function.
NIST 800-14 (2004)	3.8 Awareness and Training An effective computer security awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation.
COBIT (2007)	PO7.4 Personnel Training Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals.
Cloud Security Alliance (2010)	IS-11 Information Security Training / Awareness A security awareness training program shall be established for all contractors, third party users and employees of the organization and mandated when appropriate.
PCI/DSS (2008)	12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

Other regulations indirect security awareness requirements:
Industry or regulator prescribed

Key Drivers

Non-Employees – Customers, Partners, Suppliers

Customers and "insiders" like partners and suppliers traditionally have not been considered likely suspects in data breaches. That's changing – fast. Over the past 24 months, the number of security incidents attributed to customers, partners, and suppliers has nearly doubled.



2012 Global State of Information **Security Survey**®,

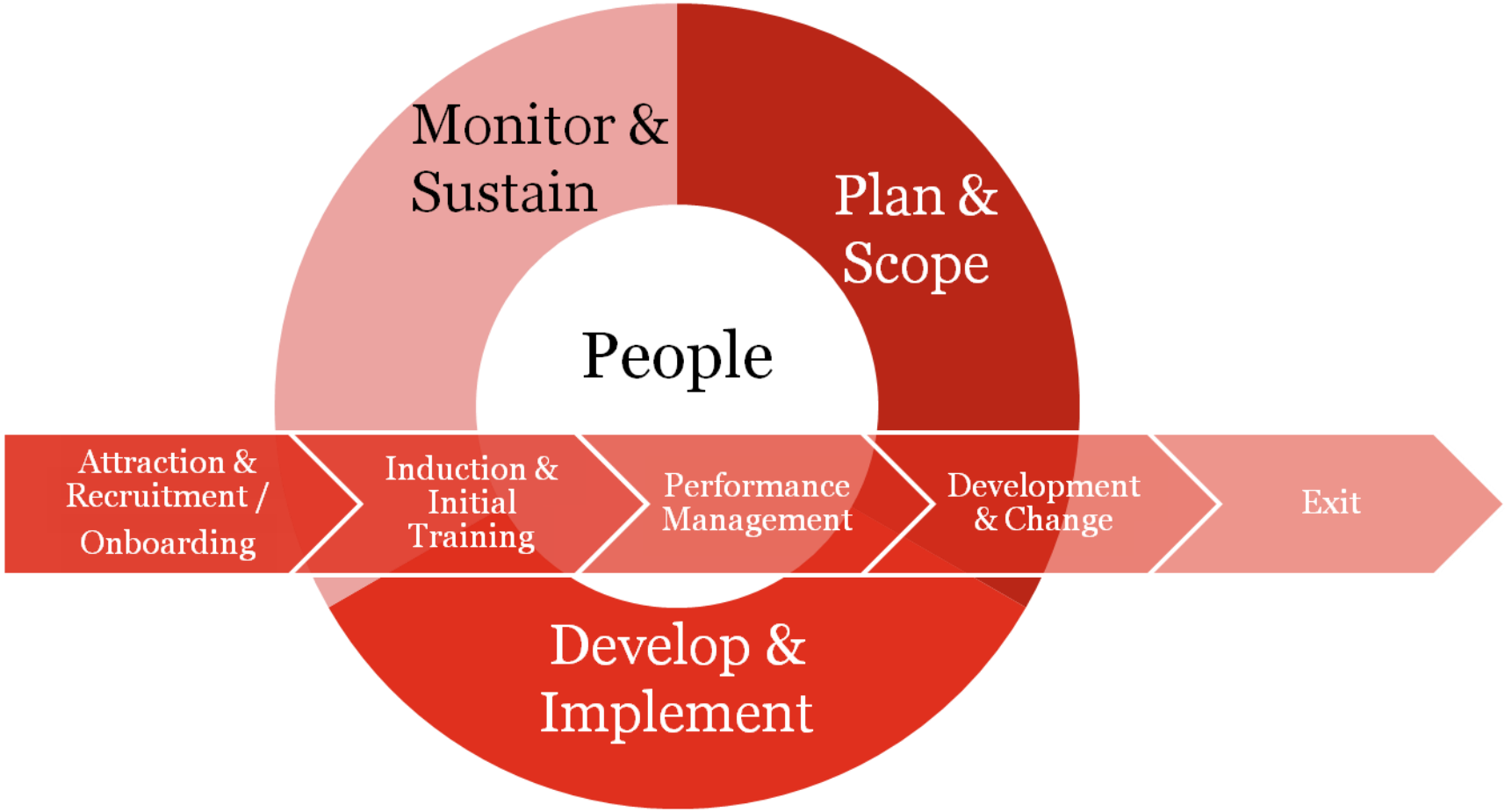
Key Drivers
Socio-Cultural Trends

- **The techno-generation -** (also termed Generation-Y) is a term used to describe a generation that has grown up within the information age (typically born after 1990) entering / entered the workplace

- **The avatar effect** - used to describe people who have difficulty distinguishing between real life and fantasy life (i.e. multiplayer online role-playing games, such as World of War-craft)….. *also sometimes leading to addictive behaviors on line gambling effecting workplace productivity as well*

Approach & Methods

Security Awareness



Approach & Methods
Security Awareness

Employee (Customer or supplier) Life Cycle Events –

- We have to ensure we re-enforce the information security messages throughout the lifecycle of the employee n(or supplier, customer etc)

Approach & Methods

Plan & Scope

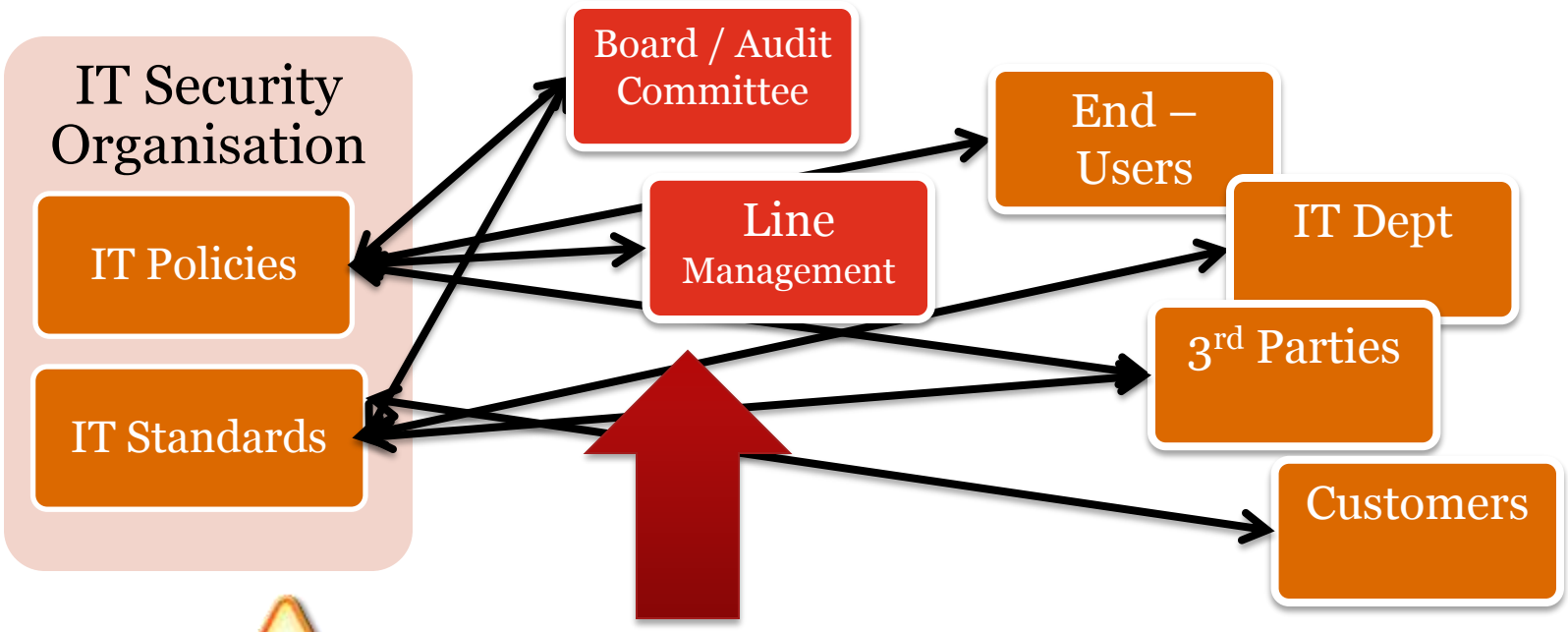
- Perform stakeholder and requirements analysis
- Identify driving and resisting forces
- Set clear and achievable objectives
- Plan to achieve objectives

Key Considerations:

- Information security policy; risk assessment results - key inputs
- Legislation/compliance requirements
- Understanding of organisational and cultural aspects including resisting forces
- Audience segmentation
- Clear management sponsorship from the beginning
- Lifecycle approach
- Team up with HR – or People & Change experts

Approach & Methods
Plan & Scope

Target audiences

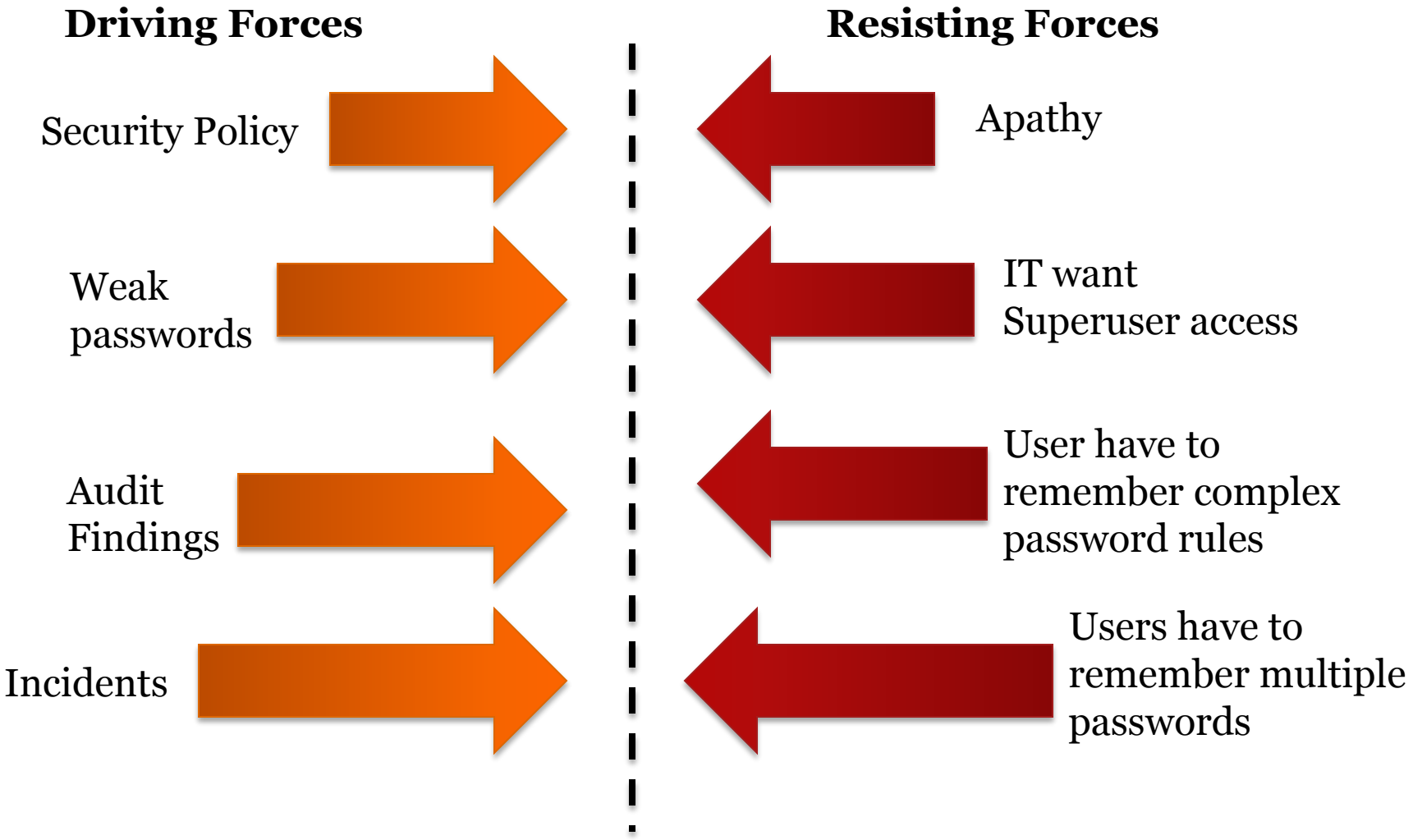


Start with these guys !

Buy-in & commitment ...it well make things easier later

Approach & Methods

Force field analysis (Kurt Lewin) & ISF



Approach & Methods
Develop & Implement

- Define security awareness messages
- Develop campaign strategy (incl. methods & frequency
- Implement strategy - deliver messages or training

Key Considerations:

- Clear "audience focused" messages delivered in a way the user can understand – use of innovative methods
- Make sure material is relevant - use "real life " case studies
- Ensure you include clear home vs work security parameters & and consequences of noncompliance for both the company and the individual
- Look for quick wins integrate with existing induction or other training or intranet sites
- Key management involvement (e.g. At introduction of training)

Approach

Develop & Implement

PwC Economic Crime Survey

- 38% of Greek Companies have not performed any cybercrime/ security training in the last 12 months / security (47% Europe & Global 42%)

- Electronic messages (e.g. email, banners) are still the most popular message delivery messages (Greece 44% Europe 36% & Global 40%)

- Seminars / Training are considered the most effective method cyber crime awareness training (Greece 44% Europe 36% & Global 40%) followed by CBT, and then emails

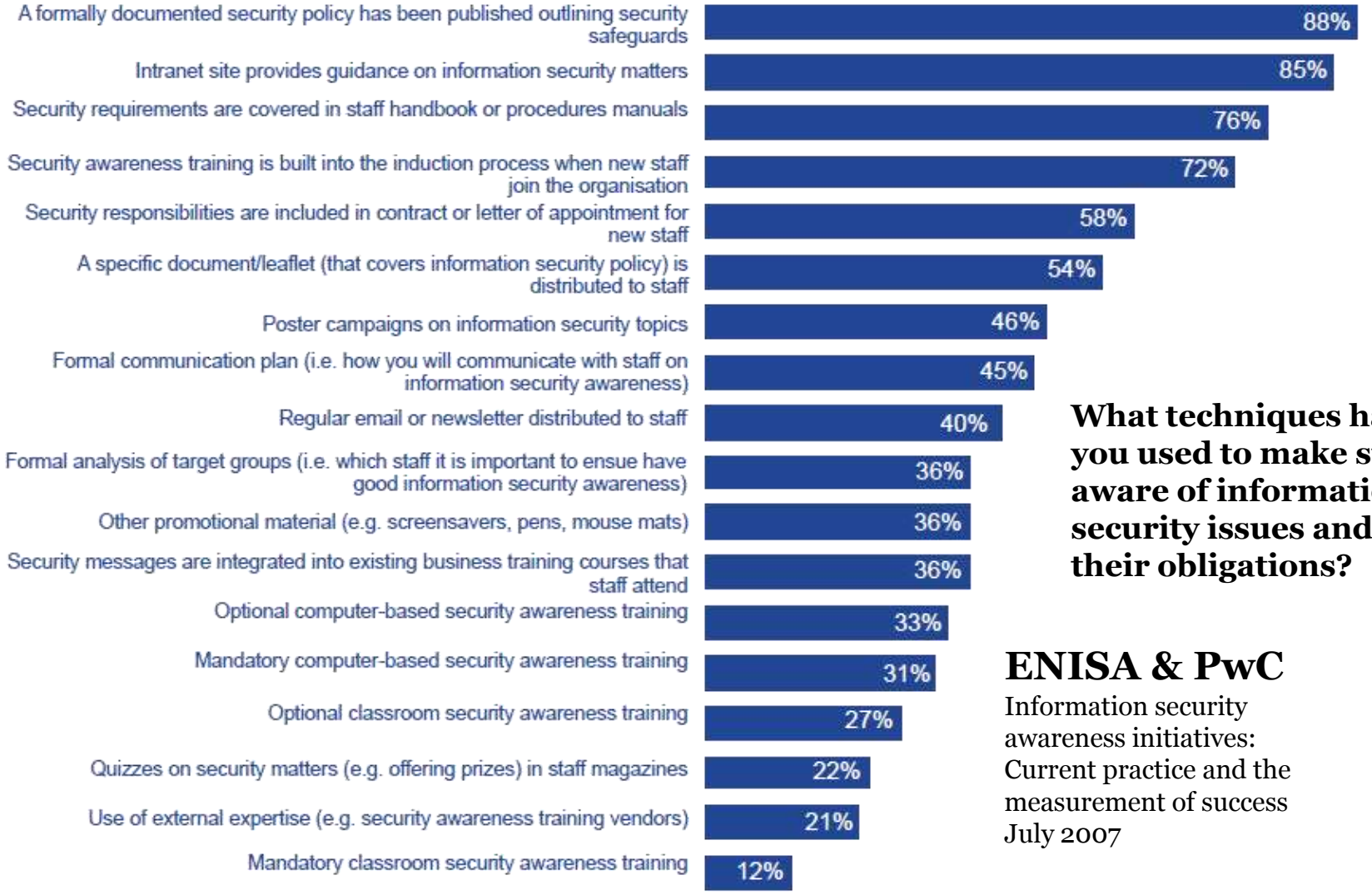
- 23% of Greek Companies use security awareness training methods (33% Europe & Global 37%) to educate users about Social media

http://www.pwc.com/gr/en/surveys/economic-crime-2011.jhtml

The 6th Global Economic Crime Survey was conducted by PwC in collaboration with Professor Peter Sommer, visiting Professor at LSE and Open University, between June and November 2011. The survey was completed by approximately 4,000 respondents from 78 countries, including Greece, and turns the spotlight on the growing threat of cybercrime.
In the context of the global survey, PwC Greece conducted its second study specifically for the country, involving a total of 92 senior executives. The study compares the results with the corresponding survey for Greece conducted in November 2009.

Approach & Methods

Develop & Implement



What techniques have you used to make staff aware of information security issues and their obligations?

ENISA & PwC

Information security awareness initiatives: Current practice and the measurement of success
July 2007

Approach & Methods

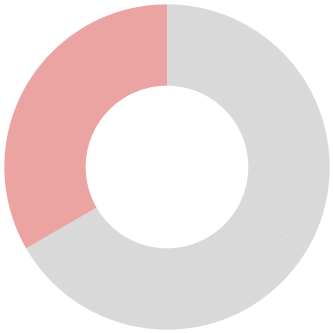
Innovative "message" delivery Ideas & Tools

Other examples:

- Log on Banners
- USB sticks
- SMS / MMS messages to company mobile phones
- Pens / MUGS
- Use of social media / videos etc

Approach & Methods

Monitor & Sustain



- Evaluate method and campaign effectiveness
- Revise & refresh
- Integrate into performance management

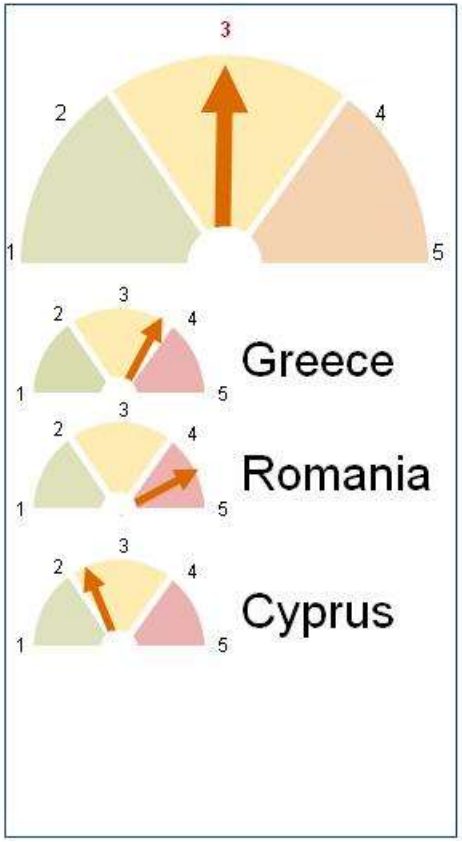
Key Considerations:

- Obtain user feedback after all training sessions
- Use qualitative metrics (users' behaviours) not just quantitative
- Maintain the momentum - revising and optimising, repeating & introducing new campaigns
- Monitor changes in compliance requirements and technology usage, risks etc - update campaigns
- Link security to personal performance objectives / appraisals
- Integrate with overall GRC program

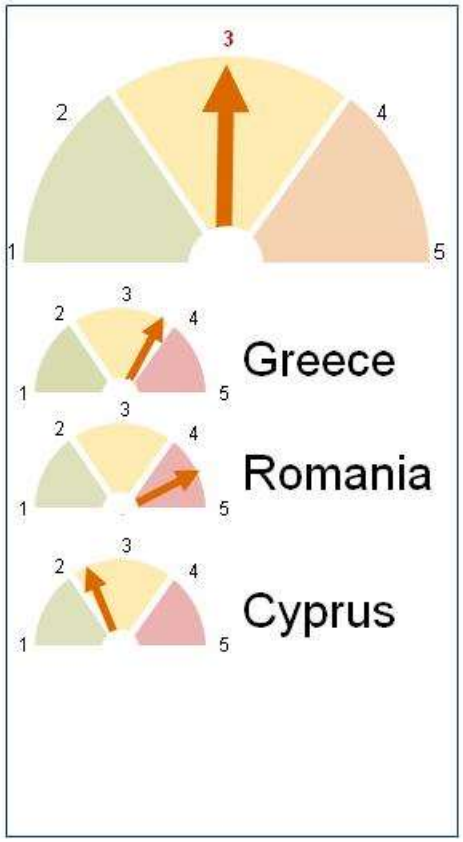
Approach & Methods

Monitor & Sustain

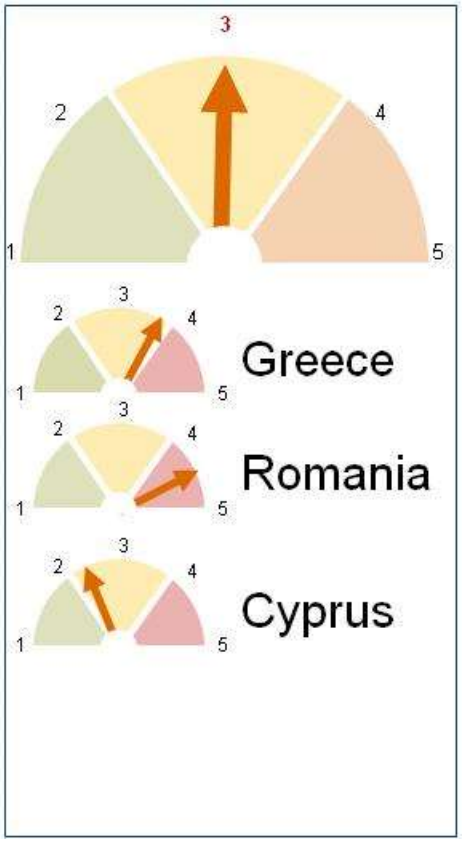
No. of Security Breaches attributable to Employees / IT Staff / 3rd Parties



No. of Internal & External Security Audit findings



No. of Staff Passed Security Awareness Testing



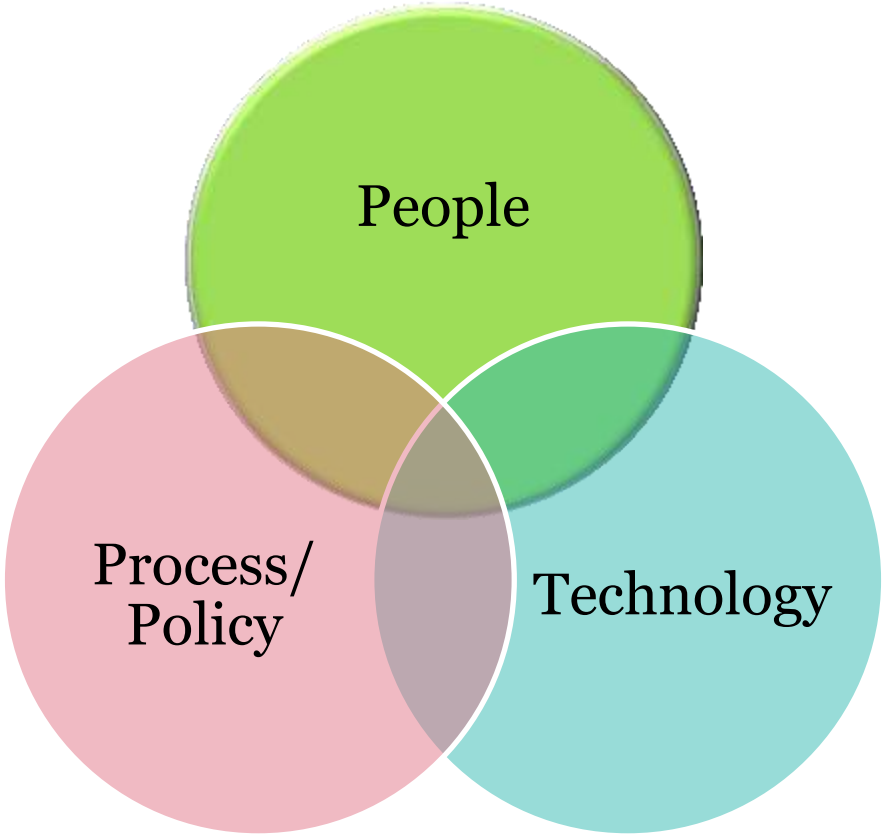
Sample Methods:

- Use of Social Engineering methods
- Use of Survey / Testing / Certification Procedures /
- Periodic Security Monitoring & Assessments

In Summary
Closing Message

A security-aware workforce will provide improved protection for an organisation's assets in a ***cost-effective*** *and efficient manner*

A robust approach to information security awareness is an effective approach to changing people's behaviour in a sustained manner and to make people the "an important line of defence.



Thank You !

Asterios (Stan)Voulanas

Partner

Technology Risk Assurance

PwC Greece

stan.voulanas@gr.pwc.com

+30 210 68 74 714