People-centric Security Awareness Program

Doctor of Business Administration Program
Muma College of Business

Federico Giovannetti | July 2021

UNIVERSITY of SOUTH FLORIDA

Intro: The problem

- Lack of employee compliance with information security policies represents a tremendous challenge to infosec practitioners.
- Enforcement leads to perceptions of infosec being an obstacle to business – The “NO” guys.
- This situation creates unproductive reinforcing behaviors where the two parties increasingly grow further apart.

Employee Behavior: Individual factors

Self-Efficacy: the belief of the individual about his/her own skills to implement a certain task
Lack of knowledge regarding the infosec policy
Lack of knowledge regarding general infosec concepts
Unintentional: stress, mood and other affects, operator error, etc.
Inertia: The manifestation of an employee's reluctance to change their current behavior
Perception of Cost vs. Benefit of compliance
Perception of the severity and certainty of monitoring and sanctions
Perception of the severity, vulnerability, and probability of security incidents

Employee Behavior: Organizational factors

Normative Beliefs: “perceived social pressure” from executives and peers who are considered as a reference point in compliance to information security policies.
Leadership support of Infosec governance. Employees tend to trust leaders with respect to policy security controls
Conflicting goals. Productivity vs. Infosec compliance. Compliance seen as impediment of business goals
Organizational commitment. How committed is the employee to the organization

Literature Review Summary/Analysis

- Most research concentrates on explaining behaviors
  - Links extensively to cognitive science
- Interventions are hard to find
  - Interesting: “hire people with the right psychological profile”
  - Lacking connection between cognitive analysis and intervention
- Organizational factors are less common in the literature
  - Management interventions seem plausible
  - Normative beliefs, group thinking, etc.

PCSAP Foundational Elements

Element	Influential Factor addressed	Intervention Component
Education	Lack of understanding of Information Security concepts	Training and simulation modules
Communication Messaging	Lack of knowledge regarding the ISP Perception of cost vs. benefit of compliance Perception of the severity, vulnerability, and probability of security incidents Self-efficacy, Inertia	Messaging tailored to show “utility” to a specific target audience and therefore engage them with the program
Leadership buy-in	Leadership support of infosec governance Normative beliefs	Message tailored to leadership to engage them to have an active role (see next item)
Leadership Message	Conflicting goals: productivity vs. compliance. Perception of cost vs. benefit of compliance	Espoused values and clear direction and priorities well communicated to organization
Ambassadors	Self-efficacy Normative beliefs Organizational commitment	Recruit the most engaged participants in the program to spread the word within their groups

Proposed Artifact

1. Segment organization into groups with common activities and goals

Executives/Officers	Sales & Marketing	Research & Development
Operations	Customer Care/Support	Product Management
Service Delivery	Finances	Information Security

2. Craft tailored message to each targeted audience
   - Considering their goals and activities
   - What matters to them, in their language
3. Recruit influencers to help deliver message
   - Leadership
   - Peers within segmented groups (ambassadors)
   - Use tailored messaging to recruit

Message Utility ➔ Awareness

Thank you!

Federico Giovannetti
fgiovannetti@usf.edu

UNIVERSITY of SOUTH FLORIDA