Fixing Security Together: Leveraging trust relationships to improve security in organizations

USEC 2015, San Diego, USA
February 8th, 2015

Iacovos Kirlappos

M. Angela Sasse

University College London

Department of Computer Science

Current Security Management in Organisations

- “*Command and control*” security

- Policies asking employees to distrust colleagues
  - e.g. no password sharing, lock screen, no tailgating

- But also don’t trust employees
  - Often security blocks their *primary tasks*
  - e.g. block access to information, control email systems
  - Reported employee concerns often not addressed

Current Security Management in Organisations

- 48% increase in security incidents in the past year alone[1]

[1] PWC. "The Global State of Information Security Survey 2015".

Trust

- Misused term in security
- *“Willingness to be vulnerable based on positive expectations about the actions of others”*
- Only required in conditions of *risk* and *uncertainty*
- Effects and potential benefits of trust on organizational security yet to be explored

Research description

- Focus: identify trust relationships
  - And impact on employee behavior
- Secondary analysis on employee interviews
  - From two large multinational organizations
  - 208 semi-structured interview transcripts
  - Employees from various lower and middle positions across organizational divisions
- Covered security awareness and compliance
  - Perception of security impact on their role
  - Appreciation of organizational support for security
  - Conditions leading to behaviors divergent from security policy

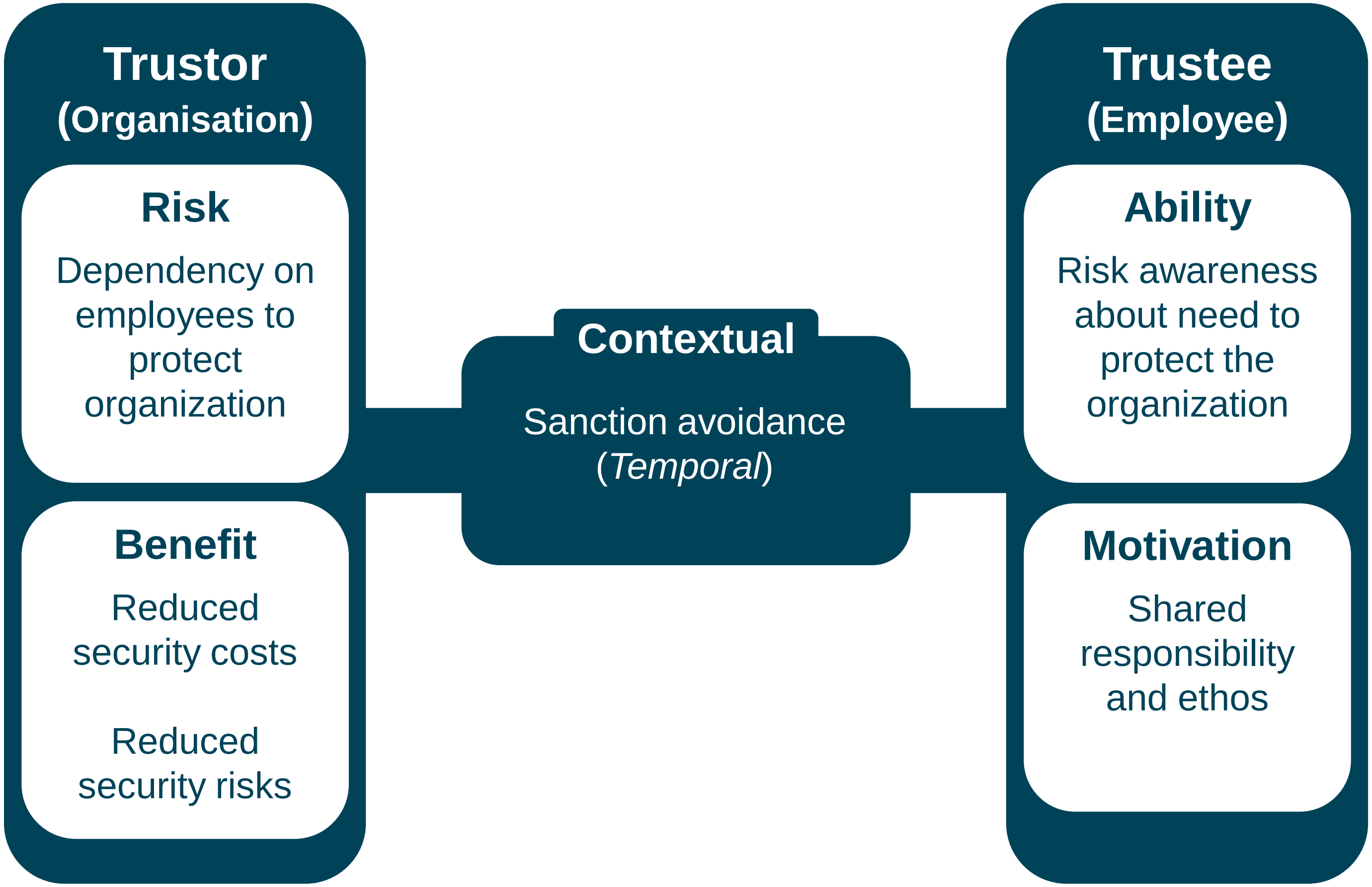
Two trust relationships

- Organization-employee trust
- Inter-employee trust
- … and conflicts between them

Organization-employee trust

- *The level of organizational dependency on the actions of employees that the existing security implementation creates*
- *“It’s almost impossible in security terms to stop a human actually attaching a document when they shouldn’t it’s very difficult to get round that.”*

Organization-employee trust



Trustor
(Organisation)

Risk

Dependency on employees to protect organization

Benefit

Reduced security costs

Reduced security risks

Contextual

Sanction avoidance
(*Temporal*)

Trustee
(Employee)

Ability

Risk awareness about need to protect the organization

Motivation

Shared responsibility and ethos

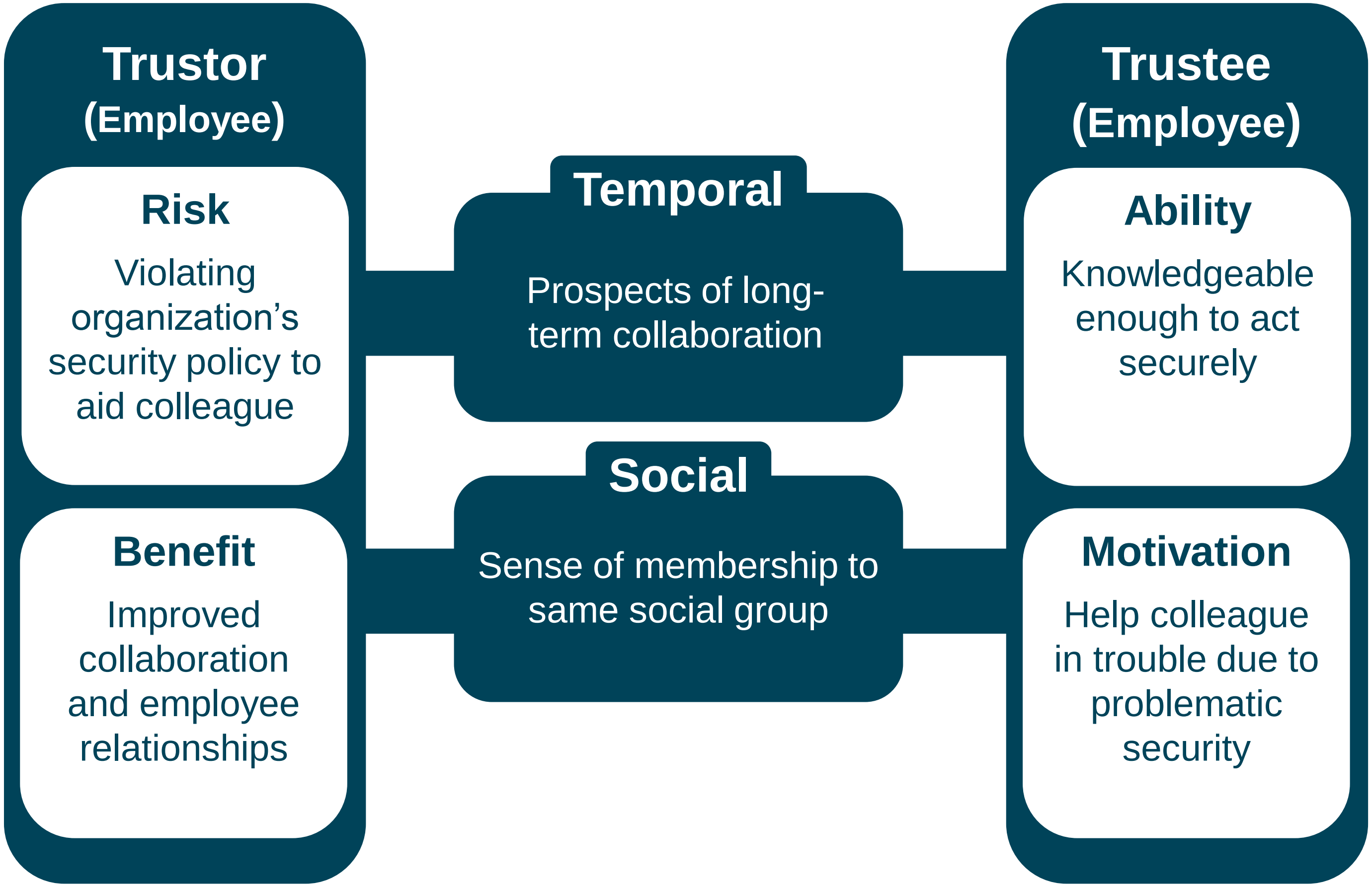
Inter-employee trust

- *The willingness of employees to act in a way that renders themselves or the organization vulnerable to the actions of another member of the organization*

- *"…because when you comment on it and say "Well you should actually be locking your screen when you walk away", the comment you get back is the fact that "Well you know we should be able to trust people around"*

- Developed both inside and outside the security domain

Inter-employee trust



Trustor
(Employee)

Risk
Violating organization's security policy to aid colleague

Benefit
Improved collaboration and employee relationships

Temporal
Prospects of long-term collaboration

Social
Sense of membership to same social group

Trustee
(Employee)

Ability
Knowledgeable enough to act securely

Motivation
Help colleague in trouble due to problematic security

Conflicts of two trust relationships

- Example: Colleague needs urgent access to an information source they are currently not authorised to access

Policy (preserve organization-employee trust)	Help colleague (preserve inter-employee trust)
Refuse help to colleague Break inter-employee trust Break colleague relationships	Help colleague (“do good”) Break organization-employee trust Face potential sanctions

- Inter-employee trust a readily-available resource to cope with over-restrictive security
  - “*Well if someone’s into the company and they need a certain document they know where to find it then pass it on*”

Risks

- Two different types of organizational security:
  - *Defined in the policy*
  - *Devised by employees on an ad-hoc basis (Shadow Security)*
- Non-compliant or ad-hoc security culture emerges
  - New employees more likely to try to “fit in”
  - Social capital development based on collective violations
  - Increasing organizational exposure to social engineering
- Breaks employee connection to the organization
  - Increasing employee incentive for collaborative non-compliance
  - Risk for insider attacks, loss of valuable human capital

Support trust development

- Simplification of security – necessary but *not sufficient*
  - *Security hygiene*: Rules should not be broken for productivity
  - "*Never give an order you know won't be obeyed*"
  - E.g. ensure online corporate file sharing locations are accessible and have adequate space
- Knowing when assurance is needed
  - When non-compliance potential rewards are high need assurance
  - E.g. use of NDAs and restricted access for high-risk projects
- Include trust in security communication
  - How real-world trust development signals break down when using computer systems (improve *ability*)
  - Explain that employees are trusted and supported in their security decisions (improve *motivation*)

Promote collective and participative security

- Put security on group meeting agenda
  - Line managers have considerable influence on staff’s security decisions
  - Employees connect with risks presented by managers/colleagues
  - Improves motivation for compliance

- Leads to *participatory security* environment
  - Increases perceived contribution and ownership of security implementation
  - Triggers internalized norms and benevolence-related compliance

Once developed, don’t enforce it!

- Avoid over-assuring
  - Employee ability and motivation to behave in a trustworthy way proven (e.g. through background checks)

- Strengthens employee ability to defend the organization
  - Attackers likely to adapt to new technologies
  - Attacks harder with suspicious and motivated employees

- *Caveat: R*esearchers and practitioners need to push for changes in regulation and information security standards

Accommodate urgency and follow it up

- Under *rare* and *unusual* conditions, employees may have to circumvent security
  - e.g. Instead of blocking emails with potentially sensitive information raise a warning – allow employee to decide
- Implement non-compliance reporting mechanisms
  - Well-defined process to alleviate resulting vulnerabilities
  - e.g. Log employee decision – follow it up
- Caveat: should not be implemented as a substitute to usable systems
  - Should be infrequent
  - Avoid non-compliance becoming part of organizational culture

Sanction violations

- Visible enforcement: Visible consequences of breaking trust

Summary

- Employees possess both *ability* and *motivation* to behave securely
- When security comes to conflict with *inter-employee trust*, non-compliance becomes only employee option
- Effective security needs a productive balance between trust and assurance
- Visible presence of trust leads to cooperation
  - Secure behavior driven by shared values and contribution to common organizational interests
  - Build social capital, goodwill, collaboration, creativity
  - Significant economic benefits
  - But breaking trust should be detectable and punishable

Future Research

- Outsourcing increasingly popular amongst large organizations
  - Impact on security-related trust development not known to date
  - Investigate how outsourcing and other changes in the organizational environment (e.g. working from home and BYOD) affect security-related trust relationships
- Test potential of mutual authentication for employees:
  - Provide mechanisms or processes for employees to authenticate to each other[2]
  - Decreasing risks from social engineering

[2] *Originally suggested by Flechais, J. Riegelsberger, and M. A. Sasse. "Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems"*

Fixing Security Together: Leveraging trust relationships to improve security in organizations