Learning from “Shadow Security”: Why understanding non-compliant behaviors provides the basis for effective security

USEC 2014, San Diego, USA
February 23rd, 2014

Iacovos Kirlappos

Simon Parkin

M. Angela Sasse

University College London

Department of Computer Science

Information Security in Organisations

- Information security threats for organisations ever-increasing
  - London-based company suffered £800 million losses (more than $1.25 billion) in intellectual property losses and contractual negotiation setbacks – (Source: MI5, 2013)

- Failings a combination of people, process and technology
  - Important to invest in all three
  - Technology strongest of the three
  - Processes well-designed
  - Researchers focus on humans as “weakest link” in security chain

Information Security in Organisations

- Policies defining security objectives
  - …and technical mechanisms required
  - …and employee responsibilities
- Assurance - Enforcing compliance
  - Limiting employee actions
  - Monitoring to identify “offenders” and sanctions for violations
- Communication through employee training schemes
  - Shape behaviour to comply with mechanisms and processes

Problems

- Impossible to comply with policies and get work done
  - Policy formulation: standards-based and past failure-driven
  - Security mechanisms sap employee resources

Problems

- Impossible to comply with policies and get work done
  - Policy formulation: standards-based and past failure-driven
  - Security mechanisms sap employee resources
- Employees do not participate in policy design
  - End-product foresees context and environment
    - employee roles, sensitivity of information, variance in threats across locations

Problems

- Impossible to comply with policies and get work done
  - Policy formulation: standards-based and past failure-driven
  - Security mechanisms sap employee resources
- Employees do not participate in policy design
  - End-product foresees context and environment
    - employee roles, sensitivity of information, variance in threats across locations
- End up as lists of “dos” and “don’ts”
  - Little effect on employee behaviour

Problems

- Impossible to comply with policies and get work done
  - Policy formulation: standards-based and past failure-driven
  - Security mechanisms sap employee resources
- Employees do not participate in policy design
  - End-product foresees context and environment
    - employee roles, sensitivity of information, variance in threats across locations
- End up as lists of “dos” and “don’ts”
  - Little effect on employee behaviour
- Prolonged enforcement of “command and control” security is unsustainable
  - Uneconomic
  - Tension between security managers and functional areas
  - “Value gap”, alienation of end-users form security

Usable security research

- Usable security: Design and build systems based on user's capabilities that fit their work environment
- Security economics improved understanding on compliance decisions
  - Influenced by own task goals, perceptions, attitudes and norms
- But…

Usable security research – Need for improvements

- Also need approaches to redesign existing systems
- Based on what employees currently do
- Security design needs to provide “middle ground” solutions
  - Balance employee and security experts’ priorities
  - Keeping organizations secure AND productive

Purpose of research

- Develop a methodology to identify high-friction security in organizational environments
- Replace it with a solution that provides a better fit with individual and organizational business processes

Identifying friction - Interviews

- 118 semi-structured interviews with employees in a large multinational organization
- Probed employees to explain their behaviour:
  - Asked about awareness and experience with corporate security policies
  - The conditions that led to the use of workarounds
  - Their responses to those conditions
  - Not encouraged to report infractions
- Analysed using Grounded Theory methodology
  - Open, Axial, Selective Coding

Results – the “Shadow Security”

- Security-conscious employees create better fitting alternatives to policies and mechanisms
- Not visible to official security and higher management
- May not be as secure as the ‘official’ policy (in theory)
  - BUT best compromise between getting job done and managing perceived risks

Results – the “Shadow Security”

- Security-conscious employees create better fitting alternatives to policies and mechanisms
- Not visible to official security and higher management
- May not be as secure as the ‘official’ policy (in theory)
  - BUT best compromise between getting job done and managing perceived risks

- “*The sum of self-made security measures created by productivity-focused employees when existing security implementation does not meet their needs*”

Shadow security drivers

1. Employee motivation to behave securely

Shadow security drivers

1. Employee motivation to behave securely
2. High security overheads
   - Time
   - Disruption
   - Cognitive load

Shadow security drivers

1. Employee motivation to behave securely
2. High security overheads
   - Time
   - Disruption
   - Cognitive load
3. Ignoring employee-reported security problems
   - Low organizational adaptability

Shadow security drivers

1. Employee motivation to behave securely
2. High security overheads
   - Time
   - Disruption
   - Cognitive load
3. Ignoring employee-reported security problems
   - Low organizational adaptability
4. Security mediation at team level
   - Attempt to moderate negative impact of security on productivity
   - Key stakeholders (e.g. line managers) are complicit in shadow security development

Risks

- Creates false sense of security
  - Employees believe they are protecting the organization
  - Risk understanding can be incomplete or inaccurate

Risks

- Creates false sense of security
  - Employees believe they are protecting the organization
  - Risk understanding can be incomplete or inaccurate
- Development of security “micro-cultures”, folk models
  - Difficult to capture
  - Reinforced by team managers and colleagues
  - Resistant to behavior change attempts

Risks

- Creates false sense of security
  - Employees believe they are protecting the organization
  - Risk understanding can be incomplete or inaccurate
- Development of security “micro-cultures”, folk models
  - Difficult to capture
  - Reinforced by team managers and colleagues
  - Resistant to behavior change attempts
- Compliance enforcement without improving usability causes disgruntlement

Lessons

- Identify and remove ‘ill-fitting’ security policies and mechanisms:
  - Usability is a *security hygiene* factor

Lessons

- Identify and remove ‘ill-fitting’ security policies and mechanisms:
  - Usability is a *security hygiene* factor

- Measure impact of security
  - On employees’ productive activity
  - …and keep monitoring it.

Lessons (2) – “Participatory Security”

- Take advantage of employees’ security capacity
  - Indicator that security solutions are not serving the business
  - Employees appreciate and play active part in provision of security
  - Include them in security design as an integral part of the process

Lessons (2) – "Participatory Security"

- Take advantage of employees' security capacity
  - Indicator that security solutions are not serving the business
  - Employees appreciate and play active part in provision of security
  - Include them in security design as an integral part of the process

- Engage with managers
  - Unique perspective on frictions between security and productivity
  - Employees turn to them for support
  - Prescribe and moderate security behavior amongst team members
  - Help them to develop correct and consistent security advice

Conclusions

- Organizations must be able to recognize
  - How when and where shadow security is created
  - How to adapt security provisions to respond to user needs
- Benefits:
  - Consistent engagement with users, provides better view of current security behaviors
  - Engages users when designing security solutions
  - Simplifies compliance
  - Post-deployment effectiveness assessment
  - Leverages team managers as security mediators and feedback providers on security-productivity friction
- An opportunity for improvements NOT a problem
  - Effective amalgamation of shadow and prescribed security

Future Research

- Currently conducting similar analyses in two organizations
  - Implement a holistic security management process.
- Deploying “shadow security driven” solutions within an organization
  - Real-world effectiveness assessment
  - Improved security decision making in industry
  - Relate behaviors to organizational metrics
- Study risk perception of employees engaging in shadow security behaviors
  - How they assess and react to risks created by their behaviors before following a course of action
  - e.g. "deleted" unencrypted files can be recovered?
- Examine compatibility of shadow security-driven information security with regulatory frameworks and international standards

Learning from “Shadow Security”: Why understanding non-compliant behaviors provides the basis for effective security