CMI Center for the Management of Information

BORDERS

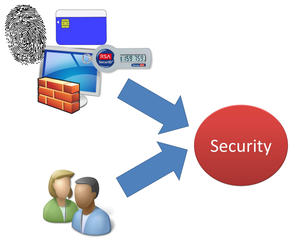
A Department of Homeland Security Center of Excellence

THE UNIVERSITY OF ARIZONA

Protecting America's Cyber Infrastructure through understanding how security controls influence humans' secure behavior

Jeffrey L. Jenkins, Alexandra Durcikova, Mary B. Burns, Jay F. Nunamaker, Jr.
Center for the Management of Information, University of Arizona

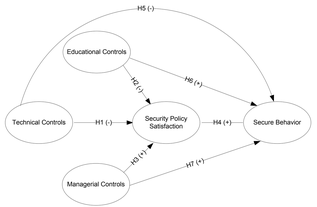
Humans are the weakest link in America's Cyber Infrastructure



We cannot ignore the interaction between controls and users in security

America's cyber infrastructure plays a critical role in the secure transportation and storage of information to prevent, mitigate, respond to, and recover from catastrophes. The weakest link in this complex system has repeatedly been shown to be the human user, who because of ignorance, negligence, or malicious intent compromises security. The purpose of this research is to examine cyber security from a human-cognition perspective. Specifically, we address how technology, education, and management controls influence a user's decision to comply with best practices for end-user computer security.

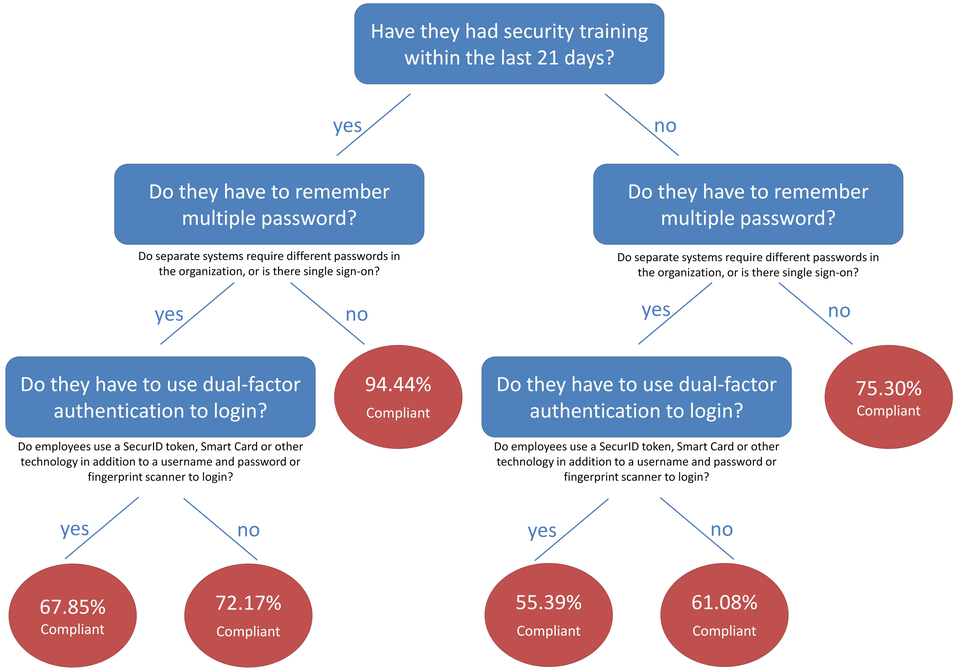
Influence of technical, educational and managerial controls on secure behavior



Hypotheses

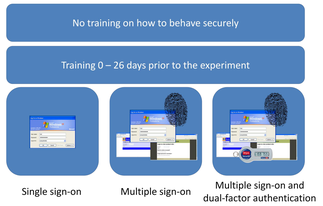
Informed by theories of human cognition and psychology, we hypothesize the intended and unintended effects of security training sessions (educational controls), the number of security safeguards implemented in a system (technical controls) and managerial support of security compliance (managerial controls) on secure behavior. Examples of technical controls can include having multiple passwords in an organization or having dual-factor authentication such as SecurID tokens and Smart Cards.

How compliant are employees with their organization's security policy?



Methodology

We conducted two laboratory experiments with 565 participants to test the influence of educational controls, technical controls, and managerial controls on secure behavior. Participants were instructed to complete a report using an enterprise-wide system. Educational controls were administered as a five minute security training video given the day of the experiment, up to 26 days prior to the experiment, or not at all. Technical controls was implemented in one of three ways—1) users had one password to access all information (single sign-on), 2) each sub-system had a separate username and password (multiple sign-on) and 3) multiple sign-on plus dual-authentication using a SecurID token. Secure behavior is defined as the degree of compliance (in %) with all aspects of a security policy commonly used in organizations. Passwords were captured and analyzed using an automated script.



Summary of Treatments

Results

Results are summarized in the center of the poster. Hypotheses are summarized below:

Summary of Results for Both Experiments

Hypothesis	Experiment 1	Experiment 2
H1. Technical controls decrease security-policy satisfaction	Supported	Not Supported
H2. Educational controls decrease security-policy satisfaction	Not Supported	Supported
H3. Managerial controls increase security-policy satisfaction	Supported	Supported
H4. Security-policy satisfaction increases secure behavior.	Not Supported	Supported
H5. Technical controls decrease secure behavior	**Supported**	**Supported**
H6. Educational controls increase secure behavior	**Supported**	**Supported**
H7. Managerial controls increase secure behavior	**Not Supported**	**Not Supported**

Acknowledgments

This project was funded through the BORDERS Center of Excellence by a grant from the Department of Homeland Security, Science and Technology Directorate, Office of University Programs.

For further information: please contact jjenkins@cmi.arizona.edu