THE NEW SECURITY CALCULUS: Incentivizing Good User Security Behavior

Sanjay Goel

Chair & Professor, Dept. of Information Security & Digital Forensics, School of Business, University at Albany, State University of New York

Kevin J. Williams, Professor, Dept. of Psychology, University at Albany, State University of New York

https://nsf.gov/awardsearch/showAward?AWD_ID=1618212&HistoricalAwards=false

Overview

- Potential vectors for data leakage from employee carelessness and noncompliance has been growing due to increased complexity of information systems, rise in personal mobile devices and third-party application, and increased contextualization of phishing emails.
- Several security interventions have failed to improve employees' security compliance, e.g., Protection Motivation Theory (PMT) and Deterrence theory (DT) both of which mainly focus on punishments and threats; these theories may not be effective since the data being protected is not personal but organizational. Additionally, these theories tend to predict more severely negative behaviors better.
- The role of extrinsic motivation in complying with information security policies is not sufficiently studied; this project explores how providing financial incentives will impact people's information security behaviors.

Challenges

- Under PMT and DT, users are expected to internally regulate their behavior based on an understanding of security threats and the consequences of risky behavior. However, users often minimize the risks associated with their behavior, rationalize noncompliant behavior (neutralization), and feel that the costs of compliance outweigh perceived benefits.
- There is a gap between user motivation and compliance. Most users do not attach an economic value to the security of their systems. Thus, instead of fear/punishment, perceived benefits may have a stronger influence for less severe behaviors (e.g., minor security policy violations).

Goals

- We propose altering user behavior and increasing compliance by changing the security decision calculus. Drawing on principles of behavioral economics, we propose providing an incentive that is powerful enough to initiate compliance, and following up with psychological manipulations (nudges) to promote ongoing internal regulation of security behavior, such that users sustain secure behaviors when incentives are no longer in place.
- Our studies will test the effects of: financial incentives, gain vs. loss framing of incentives, nudges

Studies and results

We carried out several studies to test the effect of financial incentives.

<u>Study I. Experimental study (finished)</u>

- Student participants were told that the study purpose is to validate a selection tool developed for a local company to select managers. They were asked to complete an in-basket job simulation task in which they role played as a manager in the casting/molding department of a manufacturing company and responded to emails. Among the 21 emails they received, there were three fake phishing emails.
- Students were randomly assigned to three groups: control (no incentives with security policy compliance behaviors), loss (5 dollars reserved for full compliance with money losses when violation detected), gain (up to 5 dollars gained according to the level of compliance). Participants of all groups were provided information security training at the beginning and were asked to follow the policies when applicable during the task.
- Data were collected on whether they clicked the links in the three fake phishing emails and whether they entered information on the webpages.
- The study found that incentives, either introduced with a loss or gain frame, increased individuals' alert for a non-contextualized phishing email and decreased the likelihood of clicking the link and submitting information.

<u>Study II. Field study (finished)</u>

- Twenty-four employees from a local company participated in the study. They all participated in the training session provided by the company's IT person, which reviewed company policies on protection of hardcopy documents, safe internet usage, safe email behaviors, software installation and updates, account safety, and use of removable storage. An incentive program lasting for 12 weeks started after they got familiar with company policies. Each week, each participant could gain up to 50 dollars based on their level of compliance. A feedback email on their performance from the previous week and the accumulated amount of incentives was provided weekly. Following the incentive program was a retaining period during which employees behaviors were monitored without incentives where carefully crafted nudges were provided to sustain their behavior.
- Data were collected on several metrics: 1) strength of passwords, measured with a brute-forced password cracking tool; 2) time and number of clicks on phishing emails, and whether the links embedded in the emails were clicked; and 3) number of times non-work emails were used on work computer, which was measured with users' webpage visiting log.
- The results indicate a clear shift in safe password practice and the use of non-work email due to incentives compared to the baseline security behavior. Follow-up study post incentives, during which nudges were given, showed some signs of increase in employees' non-compliance but the compliance level was higher than that before the incentive program started.

<u>Study III. Online experimental study (in process)</u>

- An online experimental study has been designed to find further support for the positive effect of financial incentives found in the first two studies.
- Participants will be recruited from online survey platforms, asked to give opinions on some legal cases stored in their personal account. Due to the sensitivity of the cases, participants will be required to change their access passwords to the system every week. The study will last for four weeks and . two to three cases will be assigned each week.
- Participants will be provided information security training and asked to comply with the policies during the study. They will be randomly assigned to one of three groups: control, gain-framing, loss-framing.
- The strength of passwords will be measured to test the effect of financial incentives.

Broader Impact

- Addressing the 'human issue' in information security could protect the privacy of users and save organizations intellectual property and reduce litigation and breach recovery costs.
- Our work will stimulate further research in behavioral security and security economics in cyber security, as well as provide a reference point for investigating human factor issues in other domains.
- The findings of the studies will be integrated in the cybersecurity courses within the BS and MS programs in Digital Forensics, and the Graduate Certificate in Information Security through the Psychology and Information Security Course.
- Four doctoral students have been directly involved in the research, acquiring research and organizational insider threat mitigation skills.
- The results of study I were submitted to a peer-reviewed journal, Information & Management and is under third round review.
- Study I and study II results were accepted by several conferences and workshops, i.e. the annual Workshop on Information Security and Privacy and the Hawaii International Conference on System Sciences