Beliefs about Cybersecurity Rules and Passwords
A Comparison of Two Survey Samples of Cybersecurity Professionals Versus Regular Users

Ross Koppel
Ph.D, FACM
Department of Sociology
University of Pennsylvania
akkriel@sas.upenn.edu

Jim Blythe
Ph.D
Information Sciences Institute
University of Southern California
byth@isi.edu

Vijay Kothari
PhD Student
Department of Computer Science
Dartmouth College
vjk@cs.dartmouth.edu

Sean Smith
PhD
Department of Computer Science
Dartmouth College
swa@cs.dartmouth.edu

"This poster is an adaptation of an earlier paper: Beliefs about Cybersecurity Rules and Passwords: A Comparison of Two Survey Samples of Cybersecurity Professionals Versus Regular Users, Security Fatigue Workshop, SOUPS 2016"

Abstract
We examine the differential perceptions of cybersecurity professionals and of general users about access rules and passwords. We conducted a small pilot study of two parallel survey instruments to elicit the perceptions and beliefs about cybersecurity policies (including who sets policy and if they include general users in that process), rationales, and compliance.

Circumvention of Access Policies is Pandemic
Often access rules make little sense to users and create barriers to performing one’s work and even to achieving the mission of the organization.

Who Sets Policy? ( Experts less clear than most users)
BIG DIFFERENCES BETWEEN GENERAL USERS AND THE EXPERTS. Most general users assumed cybersecurity policy is set by executive management or regulators (69%), and about a quarter (23%) thought it was set by local leaders. Only 15% said they didn’t know. In contrast—and very surprising given their jobs—60% of the cybersecurity professionals said they didn’t know who set the rules.

Were Users Asked When Setting Policy?
Almost half, 46%, of the general users said or strongly suspected that input from users was used in setting cybersecurity rules. In contrast, again, only 20% of the cybersecurity professionals said users’ input was used in setting these policies.

Both Cybersecurity Professionals and General Users Were Somewhat Frustrated By Rules
Neither general users nor pros were deeply frustrated by the rules; and most sought to understand the reasons for them. In fact, 23% of general users and 33% of pros were not frustrated at all.

Sensibility of Rules
How Sensible are General Rules?

When asked about management’s security rules, the two groups’ reactions were often starkly different. Pros were far more likely than general users to see the value of:
- logon rules (87% of pros see them as sensible vs. 46% of general users)
- password complexity (40% vs. 23%)
- the logic of management granting access (31% vs. 8%)

Why are Cybersecurity Rules Seen as Unreasonable?
Why are the Access Rules (Perceived as) So Foolish?

Light Rows: Asked of only general users (rows 1-3). Dark Rows: Asked of only cybersecurity professionals (rows 4-6)

Answers to these questions about the reasonableness or foolishness of cybersecurity policies offer opportunities for improvement; even if one finds users to be naive or misinformed. Only by understanding users’ perceptions can we hope to better inform them and to respond to their needs.

When people were officially taught to use a workaround

• Log on rules

44% Gen

40% Pros

60% Gen

53% Pros

When asked about management’s security rules, the two groups’ reactions were often starkly different. Pros were far more likely than general users to see the value of:
- logon rules (87% of pros see them as sensible vs. 46% of general users)
- password complexity (40% vs. 23%)
- the logic of management granting access (31% vs. 8%)

When people were officially taught to use a workaround

• Log on rules

44% Gen

40% Pros

60% Gen

53% Pros

When asked about management’s security rules, the two groups’ reactions were often starkly different. Pros were far more likely than general users to see the value of:
- logon rules (87% of pros see them as sensible vs. 46% of general users)
- password complexity (40% vs. 23%)
- the logic of management granting access (31% vs. 8%)

Conclusions

Answers to these questions about the reasonableness or foolishness of cybersecurity policies offer opportunities for improvement; even if one finds users to be naive or misinformed. Only by understanding users’ perceptions can we hope to better inform them and to respond to their needs.

While both general users and cybersecurity professionals expressed dissatisfaction with access rules and passwords, their perceptions were in some ways very different, in ways that suggest misunderstandings and misdirected approaches to improved security. This preliminary study serves as a step toward informing both cybersecurity professionals and general users to ultimately improve user behavior and cybersecurity policy. A well-informed cybersecurity professional who understands the perceptions of general users will be in a better position to address users’ concerns, to establish user trust, and to educate the user by dispelling user misperceptions and legitmizing existing (or new and better) security measures.

Limitations: This was only a pilot study. Sample sizes were very small; generalizing to larger populations is unwise. We are, however, expanding the research to larger samples and differing populations.

For more information on this and our other project work, visit http://shucs.org.