We conducted a survey to examine the differential perceptions of cybersecurity professionals (n=15) and of general users (n=13) about access rules and passwords.

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.

Different Beliefs about Users’ Involvement in 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.

Cybersecurity Rules Often Frustrate Cybersecurity Pros & Regular Users

72% of general users and 67% of pros frustrated by security rules... but seldom said they did. Pros noted: “Sacrifice in the name of security.”

\textbf{When is Circumvention Justified?}

When asked about management’s security rules, 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% v. 23%)
- The logic of management granting access (31% v. 8%)

\textbf{Cybersecurity Rules Seen as Unreasonable?}

\textbf{For General Users}

\begin{itemize}
  \item Access policies generally reasonable: 0% vs. 50%
  \item Assume policy makers not fully aware of workloads needs for as tasks: 8 vs 85
  \item Perceived lack of concern by those in charge of computer security: 8 vs 58
  \item CYBER PROS SAY: Regular users perceive Cyber Rules as a reflection of incompetence of those in charge of security: 0% vs. 43%
  \item CYBER PROS SAY: Many users see them as arrogant, users think those in charge of security feel: “I know what is best for you – don’t question my authority.” 0 vs. 36
\end{itemize}

\textbf{General Users:}

Half said security rules are generally unreasonable, although a third were less convinced. The next question is far more worrisome: 93% thought policy makers don’t understand users workflows

\textbf{Conclusions}

Understanding the perceived reasonable of cybersecurity policies offers opportunities for improvement, even if they are not misperceived. 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, they manifest many misunderstandings, and thus approaches to improving security. 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 legitimizing existing (or new and better) security measures.

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

\textbf{WHAT COMES NEXT}

Background: We have been collecting, and will continue to collect, data and insights regarding password use and misuse via surveys, observations, DASH models, Mechanical Turk experiments, interviews with cybersecurity leaders, work with Chief Security Officers, formal modeling, working with other groups and scientists to incorporate their data, and collections of passwords from published and unpublished lists and from colleagues.

Next Steps: Collect data from real world password scenarios & under realistic and differing constraints, parameters, and security needs

Systematically collect actual password reconfigurations when passwords are as a result of need or action because of required alterations to password rules, e.g., demanding special characters, additional letters or numbers, greater length, more complexity, etc. Including:

- When usernames must change because of related concerns.
- When users’ passwords are compromised.
- When users are obliged to create new accounts or increase security on existing accounts, e.g., use of two-factor authentication, need to create new account because of mergers, etc.
- When obliged to provide or alter security questions.

\textbf{Experiment: Two data collection methods}

1. “Naturally occurring data” from events where users create or alter existing credentials, as outlined above—parts of natural occurrences (and thus “natural experiments”) wherein organizations confront their increasing awareness and the reality of cyber threats by imposing new password rules or otherwise instructing their users to change their credentials.

2. Data gathered in response to password rules that change we partially or wholly help formulate, e.g., by cooperating with existing organizations that wish to increase security or change existing systems. That is, we shall design our interventions with cooperating cybersecurity leaders in participating organizations to enact changes that allow us to best understand and document password behaviors.

We then could observe what happens when users are instructed to create passwords in response to different password composition policies:

- 25% of users are instructed to create new passwords without guidance.
- 25% are required to create passwords that comply with a stringent password composition policy.
- 25% are required to create passwords that comply with a lax policy, and
- 25% are forced to use two-factor authentication.

Note that in no case would we ever know the usernames associated with any users. Each user will be assigned a random number for our datasets so that we can follow the trajectory of changes but never know the identity of the user.

\textbf{Additional Experiments & More Findings}

- Alternative password strength indicators and feedback mechanisms (e.g. with user-friendly guidance vs. other systems);
- Rules about affiliations between passwords and user names (via-a-vis repetition of terms) or passwords and name of service or organization (e.g., password cannot incorporate name of URL or organization);
- Passwords that can or cannot include elements of the previous passwords (e.g., Fluffy1, Fluffy2, Fluffy3, etc.), and so on.

\textbf{OUTCOMES, LESSONS, FINDINGS}

1. Provide real life datasets on how people understand password rules, how they respond to rules, how they conceptualize security in use; how passwords are changed to reflect new rules
2. Embracing enrich DASH password modeling efforts, Mechanical Turk parameters, & many simulations and models
3. Building theoretic and empirical basis for the science of security
4. Provide direct practical value for cybersecurity protection.