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

Ross Koppel
Department of Sociology
University of Pennsylvania
rkoppel@sas.upenn.edu

Jim Blythe
Information Sciences Institute
University of Southern California
blythe@isi.edu

Vijay Kothari
Department of Computer Science
Dartmouth College
vijayk@cs.dartmouth.edu

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

ABSTRACT

In this paper we explore the differential perceptions of cybersecurity professionals and general users regarding access rules and passwords. We conducted a preliminary survey involving 28 participants: 15 cybersecurity professionals and 13 general users. We present our preliminary findings and explain how such survey data might be used to improve security in practice. We focus on user fatigue with access rules and passwords.

1. INTRODUCTION

If designers and administrators of computer systems have different understandings of the purpose and value of access rules compared to the actual users of those systems, then the utility of those rules will be continually challenged. Circumvention of access policies is pandemic—often because the rules make little sense to users and because they create barriers to performing one's work and achieving the mission of the organization. To examine the differential perceptions and efficacy of cybersecurity policies, we created two parallel survey instruments to elicit the perceptions and beliefs about cybersecurity policies, rationales, and compliance. One instrument was administered to cybersecurity professionals and one to regular users of IT systems—generally employees in firms or upper-level students who also held computer-related jobs. Most questions were identical except in a few instances where changes were required by the respondents' roles.

The findings and comparisons address the frequent circumvention of password and access rules—focusing on password creation and use. Our research is designed to inform questions about why security policy is often misdirected and why it sometimes generates unintended consequences such as security fatigue-induced circumventions—resulting in a greater attack surface instead of greater protection.

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22-24, 2016, Denver, Colorado.

1.1 Background

User behavior is often at odds with security objectives, not because users are inherently bad, but because even good users subjected to fatigue-inducing security practices will be motivated to circumvent them (e.g., [1,2]). Indeed, numerous studies are centered on understanding users' behaviors, users' motivations to engage in those behaviors, and security fatigue---including frustration and workflow impediments---that induces circumvention, many of which are concerned with passwords and access control (e.g., [3,4,5,6,7,8,9,12]). If there's one thing to be learned from this research it is that security must be usable! The impetus for deploying usable security policies, mechanisms, and systems has led researchers to explore both general users' and cybersecurity professionals' mental models and to study the differences amongst these mental models and reality (e.g., [10,11]). We build upon the existing literature by acquiring and analyzing new survey results on the differential perceptions of cybersecurity professionals and users regarding passwords and access rules.

1.2 Methodology

We administered surveys online via Survey Monkey and collected results. We obtained only pilot samples (N = 15 cybersecurity professionals; 13 general users). In the context of this paper, "cybersecurity professionals" are people involved as computer system administrators and security policy creators. "General users" are usually students, although some had held jobs in IT and in IT security (see "Limitations discussion"). In the two convenience samples, cybersecurity professionals were solicited at cybersecurity meetings while general users were students or workers whom we did not know to be involved in cybersecurity tasks (see surveys in appendix).

Even though these are clearly only pilot-level samples, we note the two instruments were pretested and modified over 15 iterations each. Each was also reviewed by at least 5 experts in the field. The surveys were approved by the IRB at the University of Pennsylvania (home institution of the lead author).

2. POLICY CREATION

Our initial questions dealt with perceptions of how user-side security policy was created.

2.1 Whose Policy?

When asked **"Who sets policy about access to the computers and systems (e.g., desktops, network, laptops, servers) you use**

most often in the course of your work?" we received similar responses between the two groups, although cybersecurity professionals were three times as likely as general users to emphasize the role of "professional or industry rules." Most said senior security or IT staff set it on an enterprise-wide level. Other options, which generated few responses, were: "No idea," "Individual workplace units," or "regulators."

2.2 Whose Logic?

When asked about the *basis (logic or rationale)* for setting your organization's *policies* on computer access rules**,** most general users assumed it was set by executive management or regulators (69%) and a few thought it was set by local leaders (23%). Only 15% said they didn't know. In contrast—and remarkable given their jobs—60% of the cybersecurity professionals said they didn't know who set the rules.

2.3 Users Asked?

We then asked whether users were asked for input on cybersecurity rules. Almost half, 46%, of the general users said or strongly suspected that input from users was used. In contrast, only 20% of the cybersecurity professionals said users' input was used in setting policy. That is, users were more likely to assume their input was considered in setting policy than those involved in setting those policies.

3. FRUSTRATION ABOUT ACCESS POLICIES

The next question and comparison is about frustration. It has two slightly different introductory sentences, although the answer options are identical. The general user introductory sentence reads: "some of us are frustrated by access policies that appear restrictive and may interfere with our work." The cybersecurity professional introductory statement reads: "many of us are frustrated by access policies that seem to provide little if any security benefit, and are also non-responsive to the needs of users who are trying to do their jobs." Respondents rated their frustration on a Likert scale from 1 to 5 where 1 = "Not frustrated, policy seems reasonable" to 5 = "Very frustrated, policy seems arbitrary or not responsive to workflow needs."

Respondents in both groups were generally not that frustrated. However, general users were overall less delighted by security rules.

Subjects from both groups provided additional comments regarding their frustrations, including specific examples of frustrations. Cybersecurity professionals' comments were:

- "Having to login every time"
- "The requirement to change the password every 70 days."
- "Getting logged out because of timing when you're in a rush."
- "Waiting so long when turning on/off the computer as it decrypts/encrypts information."
- "Unplanned system downtime frequent mandatory password changes."
- "Having to retype my password all the time."
- "Sometimes the authentication is done with my real name; sometimes it's done with an arbitrary username I selected and sometimes it is done with [Enterprise name] ID. I often forget which is which."
- "Sometimes, there are no access to Internet and sometimes the speed is extreme slow."
- "Worrying about our servers or networks which are not protected (lab or dorm networks) being compromised."
- "Recalling multiple passwords each with different complexity rules."
- "Some workstations don't allow executable files to be run."

General users' comments were remarkably similar in tone and levels of frustration:

- "The work is delayed."
- "Sync'd credentials means that if I submit my credentials to an attempted phish, the bad guys could access more than just email, and it's bad enough when they just access email because our institution gets blacklisted and no one's email gets sent/received."
- "Passwords regularly forgotten (because they have to be changed). Delay in work (because password has changed). Confusion about usernames and passwords (multiple accounts and/or passwords) Confusion about internal and external accounts (for example Microsoft business and private accounts)."

Table 1. Frustration about Access Policies

	1 (Not Frustrated)	2	3	4	5 (Very Frustrated)
General users	23%	39%	15%	23%	0
Cybersecurity professionals	33%	27%	33%	7%	0

Table 2. How Well Thought Out is the Access Policy?

	1 (Thoughtfully Developed)	2	3	4	5 (More of a hindrance than anything else)
General users	23%	38%	31%	8%	0%
Cybersecurity professionals	40%	47%	7%	7%	0%

- "New employees can wait a week before full access to needed resources (training time lost) Parents frustrated because cannot pay tuition bill online until student grants parent access (FERPA) Alumni frustrated because they need an online account created by IT in order to request a transcript from Registrar. Off-site employees frustrated because their supervisor needs to request VPN and other access on their behalf."
- "I have seen people attempting to log in on public University computers and swearing that they are typing in their password correctly but are unable to access the system."
- "Frustration. Not able to do their job. Give up or don't care anymore."
- "Work delayed: 2 extra minutes like 10 times a day is true. Hate using the system. My boss says this about salesforce and deskflex."
- "I don't buy the assumption that there is an adverse effect [to cyber security]. Surely a compromised work station or exposure of sensitive data has a greater effect on productivity"?
- "Frustration, Yes, but they are constrained by some laws (FERPA, Wage laws) and constraints of supporting BYOD."

4. SENSIBILITY OF POLICY

4.1 How Well Thought Out is the Access Policy?

We asked both groups: **"Even if you are frustrated by the access policy, do you see it as necessary to protect security, or do you see it as not well thought out, where the security benefit is less than the effort required to comply?"** General users were less likely than cybersecurity professionals to view access policies as well-thought out; although no one insisted they were meaningless.

4.2 How Sensible are the Several Rules?

When asked about management's rules regarding the many cybersecurity rules, the general users' reactions and cybersecurity professionals' reactions are often starkly different. General users' percentages are shown as the first number in each cell; the second number is the percent for cybersecurity professionals.

Cybersecurity professionals are 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%) and the logic of management granting access (31% v. 8%). Cybersecurity professionals also wrote additional comments that amplify (or contradict) the fixed-choice items. These cybersecurity professionals wrote:

- "I have to manually open doors for people from other departments, who need access to our department for meetings if someone forgets a password, it takes a long time to reset it (several hours), so time is lost"
- "Some regulations came from outside of the country and didn't quite take into consideration the local business sector. The directive of not sharing passwords / resources was also often ignored to get business done faster or remotely. People were however good about keeping client information secured, and using encryption for their devices and emails."
- "Users write down certain passwords, because they are impossible to remember (they are set by the system rather than [by] users)"
- "VPN server often denies overseas access and require user to

Table 3. How Sensible are Several Rules?

	Generally Sensible		Sometimes Sensible		Not Sensible		Don't Know	
	Gen	Pros	Gen	Pros	Gen	Pros	Gen	Pros
Log on rules	46%	87%	46%	0%	8%	13%	0%	0%
Password rules for different passwords for each app	30	7	20	53	50	27	0	13
Password complexity	23	40	38	20	38	40	0	0
Password change frequency	25	13	58	40	17	33	0	13
Management's rules on granting access	8	31	69	23	15	8	8	38
Inactivity timeouts	31	53	54	33	15	13	0	0
Different rules for different systems	17	21	42	43	33	14	8	21
Rules by how/why access is provided	38	53	46	20	15	13	0	13

Table 4. Circumvention Justifications

	General Users	Cybersecurity Professionals
Critical task, e.g., saving a life, keeping the grid up	83%	79%
When the rules are so foolish that nothing else makes sense	42%	57%
Access associated with role(s) make no sense, e.g., members of the same team can't see all of the information because only some have official access	17%	36%
When allocation of access is foolish, e.g., people hired before November have access but others with similar functions and responsibilities don't	28%	9%
When everyone else is circumventing a specific rule	58%	43%
When people were officially taught to use a workaround	58%	71%

call IT help desk in different time zone."

- "It's too hard to comply: Lots of users don't comprehend passwords requiring case switching or switching passwords every thirty days. They can't comply with log-ins for username and password"
- "In some systems, if you change the whole API to log in, it may cause many potential problems for old users."

For comparison, the general users wrote:

- "Our institution has a requirement to encrypt sensitive data stored locally and requires permission from a data owner. Alternatively, all sensitive data is permitted to be stored on institution servers. In general it's easy to comply by storing such data on a share and people general do, even when they 'have' to get permission to store it elsewhere."
- "Password and account sharing."
- "Saving sensitive data on personal hard drive."
- "Shared passwords because people don't want to ask how to delegate access to such things as calendars or cloud storage. Easy to do but requires asking or taking a few minutes to type the question into a search box."
- "Making passwords easy to guess by using alternate spellings to work around the dictionary rule. For example 'boyz' instead of 'boys' or 'bux' instead of 'bucks'"
- "1) system admins routinely ignore requirement to use separate admin accounts instead of their own account to manage systems. 2) sharing of account credentials to facilitate workflow 3) Don't change passwords and re-use passwords 4) Retain rights longer than necessary (say after a job change, they keep privileges no longer needed) "
- "Logging on to system applications to sign on to server, using time sheets, schedule rooms, kiosks, client web portals to assist with service questions."

5. CIRCUMVENTION JUSTIFICATIONS

We asked general users and cybersecurity professionals: **"When do you think most personnel would find circumvention of the access rules is justified? (Check as many as applies.)"** The answers are often similar—revealing the widespread awareness of circumvention and the rationales for it.

Cybersecurity professionals appear more aware than are general users of justifications for circumvention of access rules associated with the need for team-wide access and when users are taught the circumvention as part of their training. On the other hand, those pros seem less aware of many other justifications for circumvention, e.g., when rules make no logical sense to the users.

5.1 Why are the Access Rules (Perceived as) So Foolish?

We asked both general users and cybersecurity professionals questions about why so many users find access rules unreasonable. The question introduction reads: "**If people have a theory or belief about why the access rules may appear non-responsive to workflow needs, is it (can indicate multiple reasons)."** As seen in Table 5, both general users and cybersecurity professionals received three common questions; additionally, three questions were asked only of general users and one was asked only of cybersecurity professionals." Looking, at the first row, we see half of general users say security rules are generally reasonable, although a third report that such sanguine views are unwarranted ("unlikely"). Responses to the next question are even more disappointing. We asked general users if policy makers might not be fully aware of the workflow needs for all tasks? More than 9 out of ten (93%) report this is likely or very likely. Similarly, (row 3) almost three-fifths of general users report that those in charge of security are not concerned about general users.

Turning to the question asked only of cybersecurity professionals (row 4), we see that about two-fifths of them indicate they are likely viewed as "incompetent," by the users they are charged with protecting. On the plus side, most, two-thirds, say it's unlikely that the security chiefs are viewed as incompetent; and

Table 5. Why are the Access Rules (Perceived as) So Foolish?

Light Shaded Rows: Asked of only general users (rows 1-3); Dark Shaded Rows =only cyber security professionals (row 4)

	Very Likely Gen Pros	Likely Gen Pros	Unlikely Gen Pros	Don't know Gen Pros	NA: Responsive Rules: Gen Pros
1 Not applicable: Users find access policies generally reasonable (**asked only of gen. users**)	0% ^	50% ^	33% ^	16% ^	0 ^
2 Users may assume policy makers not fully aware of workflow needs for all tasks (**gen users only**)	8 ^	85 ^	8 ^	0 ^	0 ^
3 Perceived lack of concern by those in charge of computer security (**asked only of gen. users**)	0 ^	58 ^	42 ^	0 ^	0 ^
4 Perceived incompetence of those who are in charge of security (**only asked of pros**)	^ 0%	^ 43%	^ 57%	^ 0%	^ 0%
5 Perceived arrogance of those who are in charge of security ("I know what is best for you – don't question my authority…")	8 0	43 36	50 64	0 0	0 0
6 Externally-imposed regulations which do not appear to be reasonable, dictating access rules	33 14	17 36	42 36	8 14	0 0
7 Using security as an excuse for laziness, e.g., they should fix something but just say it must be as is because of "security"	17 0	25 20	58 53	0 27	0 0
^ = question(s) not asked of that group					

none said such negative perceptions were "very likely" to be the case.

The last three rows—where we can compare both groups' responses--offer some similarities and occasionally strong contrasts between the general users and the cybersecurity professionals. General users are slightly more likely than the pros to view security chiefs as "arrogant" (row 5). There is no clear pattern about the perceptions about externally imposed security rules. However, the last row (7) reveals that general users are considerably more likely than the pros to say cybersecurity staff use claims of "security" as an excuse to justify delays or refusals to fix problems or make changes.

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

6. DISCUSSION

These findings illustrate widespread disappointment with current cybersecurity policies—a perception shared by both cybersecurity professionals and general users. Both groups expressed significant frustration and a sense of powerlessness over who created the rules and the ability to change them in positive ways. That said, there are clear differences in understandings and perceived solutions, often in unexpected directions. Cybersecurity professionals, for example, were more likely than general users to say they didn't know who set access rules, but they were more certain that the rules did not reflect user input. Both groups were often frustrated by access policies, and expressed long lists of examples. On the other hand, the security experts were far more likely than the general users to say that access policy was thoughtfully developed and sensible.

Both groups can easily envision conditions where they would circumvent security rules (e.g., saving a life or keeping the grid up).

Limitations: We reiterate that this is a preliminary study with a small sample size. Also, separation of the samples—as cybersecurity professionals vs. general users—is sometimes fuzzy. Also, for some items, respondents may be differentiating between their own views and their expectations of others' views. We aim to extend sample sizes and selection processes, and perform further analyses that can be used to inform cybersecurity professionals.

7. CONCLUSION

We explored the perceptions of general users and cybersecurity professionals regarding access rules and passwords. While both groups 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 legitimizing existing (or new and better) security measures.

8. ACKNOWLEDGMENTS

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Maryland Procurement Office. Koppel's work was supported in part by NSF CNS-1505799 & the Intel-NSF Partnership for Cyber- Physical Systems Security & Privacy.

9. REFERENCES

[1] Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46.

[2] Blythe, J., Koppel, R., & Smith, S. W. (2013). Circumvention of security: Good users do bad things. *IEEE Security & Privacy*, (5), 80-83.

[3] Florencio, D., & Herley, C. (2007, May). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (pp. 657-666). ACM.

[4] Florêncio, D., Herley, C., & Van Oorschot, P. C. (2014). Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *23rd USENIX Security Symposium (USENIX Security 14)* (pp. 575-590).

[5] Gaw, S., & Felten, E. W. (2006, July). Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (pp. 44-55). ACM.

[6] Hoonakker, P., Bornoe, N., & Carayon, P. (2009, October). Password authentication from a human factors perspective: Results of a survey among end-users. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 53, No. 6, pp. 459-463). SAGE Publications.

[7] Riley, S. (2006). Password security: What users know and what they actually do. *Usability News*, *8*(1), 2833-2836.

[8] Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., ... & Cranor, L. F. (2010, July). Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2). ACM.

[9] Sinclair, S., & Smith, S. W. (2010). What's Wrong with Access Control in the Real World?. *IEEE Security & Privacy*, (4), 74-77.

[10] Smith, S. W., Koppel, R., Blythe, J., & Kothari, V. (2015). Mismorphism: a Semiotic Model of Computer Security Circumvention. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)* (p. 172). Lulu. com.

[11] Wash, R. (2010, July). Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 11). ACM.

[12] Whalen, T., Smetters, D., & Churchill, E. F. (2006, April). User experiences with sharing and access control. In *CHI'06 extended abstracts on Human factors in computing systems* (pp. 1517-1522). ACM.

A. SURVEYS

Below, we provide both the survey we administered to general users and the one we administered to cybersecurity professionals.

A.1 Survey for General Users

The survey for general users begins on the next page.

ShucsSurvey 3

Anonymous Survey about Computer Access Frustrations v4

The purpose of the study: To understand workers' frustrations and workarounds about access to computer systems. That is, we ask about barriers or inconveniences confronting personnel who seek to perform work they are supposed to accomplish. Personnel are sometimes denied access because of problems such as lost passwords, required password changes, forgetting a specific log-on name, altered rules, system breakdowns, need to access the system via a different computer than usually used, etc. It is not a study of hackers or those with malicious intent.

Your participation in this research study is voluntary. If you decide not to participate, you are free to stop at any time. Withdrawal will not interfere with your work or with your organization. If you have questions about your participation or rights in this research, you can discuss them with the study investigator or members of the study team. You may contact Prof. Ross Koppel, Ph.D. at the University of Pennsylvania at: rkoppel@sas.upenn.edu.

1. Which “industrial” sector best describes the principal business area of your organization? (Note that we do not ask for the name of your organization or any identifying information.) You may check more than one category.

- □ Agriculture, Forestry, Fishing and Hunting
- □ Mining, Quarrying, and Oil and Gas Extraction
- □ Utilities (electricity, water, waste treatment, etc.)
- □ Construction
- □ Manufacturing
- □ Wholesale Trade
- □ Retail Trade
- □ Transportation and Warehousing
- □ Information Technology
- □ Finance and Insurance
- □ Real Estate and Rental and Leasing
- □ Professional, Scientific, and Technical Consulting Services
- □ Management of Companies and Enterprises
- □ Administrative & Support & Waste Management & Remediation Services
- □ Educational Services
- □ Health Care and Social Assistance
- □ Arts, Entertainment, and Recreation

2. How would you define your role at your organization (may check more than one box, but indicate if that is your primary role):

	Yes, Primary	Yes, Secondary
I use computers to get my job done – but I'm not an IT professional	○	○
I work on the help desk in the IT Dept. of my organization	○	○
I'm part of the IT team that addresses requests for modifications/fixes	○	○
I'm a computer consultant working here	○	○
I write or maintain software or hardware here	○	○
I train staff on IT subjects	○	○
I sell software or hardware (I work for a vendor)	○	○
I work as a technician in the IT Dept of my organization	○	○
I help set computer security policy for my organization	○	○
I work in an administrative role in the IT Dept (e.g., office manager).	○	○

Other (please specify)

3. Who sets policy about access to the computers and systems (e.g., desktops, network, laptops, servers) you use most often in the course of your work?

□ No idea

□ Individual workplace unit (e.g., my dept or my boss)

□ Senior security or IT staff - Set at organization-wide level

□ Regulatory rules (rules set by regulators)

□ Professional or industry rules (e.g., all engineers will password protect…)

Other (please specify)

4. To the best of your knowledge, are your organization's policies on computer access based on: (Check all that apply):

□ Don’t know

□ Systematic analysis of use patterns,

□ Local rules set by local leaders

□ Rules set by executive management, political rules, regulators, etc

Other (please specify)

5. Do those who set security policy on access ask for input from users?

○ Yes

○ Not sure, but suspect it's yes.

○ Not sure, but suspect it's no

○ No

○ Don't know

Comment

6. If "Yes" to above: To the best of your knowledge, was your input considered?

○ Yes

○ Not sure, but suspect it's yes.

○ Not sure, but suspect it's no

○ No

○ Don't know

Comment

7. Some of us are frustrated by access policies that appear restrictive and may interfere with our work. On a scale from 1 to 5, where 1 = “Not frustrated, policy appears to be reasonable” to 5 = “Very frustrated, policy seems arbitrary or not responsive to workflow needs,” please indicate your assessment:

1 (Not Frustrated)	2	3	4	5 (Very Frustrated)
○	○	○	○	○

Other (please specify)

8. Even if you are frustrated by the access policy, do you see it as necessary to protect security, or do you see it as not well thought out, where the security benefit is less than the effort required to comply.

1 (Thoughtfully developed)	2	3	4	5 (More of a hindrance than anything else)
○	○	○	○	○

9. If people have a theory or belief about why the access rules may appear non-responsive to workflow needs, is it (can indicate multiple reasons):

	Very Likely	Likely	Un-likely	Don’t know	NA. Rules responsive
Not applicable: Users find access policies generally reasonable	○	○	○	○	○
Users may assume policy makers not fully aware of workflow needs for all tasks	○	○	○	○	○
Perceived lack of concern by those in charge of computer security	○	○	○	○	○
Perceived arrogance of those in charge of security (“I know what is best for you – don’t question my authority…”)	○	○	○	○	○
Externally-imposed regulations which do not appear to be reasonable, dictating access rules	○	○	○	○	○
Using security as an excuse for laziness, e.g., they should fix something but just say it must be as is because of “security”	○	○	○	○	○

Other (please specify)

□

10. In general, please indicate how these access rules (see below) are perceived by most people in your organization. (Select a button for each and/or write an explanation in the "It's Complicated" box.)

	Generally sensible	Some-times sensible	Not sensible	Don’t know
Log-on rules	○	○	○	○

It’s complicated, Please explain…

□

	Generally sensible	Some-times sensible	Not sensible	Don’t know
Need to use different passwords for different applications	○	○	○	○
It’s complicated, Please explain…				
Passwords—Complexity	○	○	○	○
It’s complicated, Please explain…				
Passwords change frequency	○	○	○	○
It’s complicated, Please explain…				
Access granting practices used by management	○	○	○	○
It’s complicated, Please explain…				
Inactivity- timing out rules	○	○	○	○
It’s complicated, Please explain…				
Systems with different access rules	○	○	○	○
It’s complicated, Please explain…				
Who gets access & why	○	○	○	○
It’s complicated, Please explain…				

ShucsSurvey 3

Question 11, Introduction:

Often, restricting access to legitimate users has unintended consequences for the organization. Obviously, there are tradeoffs between access and security; it's very hard to get it right for all settings. Here are examples of unintended outcomes from restricting access.

>Patient harmed because access to medications denied
>Work delayed or lost
>Colleague dismissed
>Requires 2 extra minutes ~34 times a day
>Makes me hate this system
>Prevents teamwork because we all need simultaneous access

11. Now, please briefly tell us of unwanted outcomes you may have heard about because of restricted access to legitimate users. (Can include examples from above, also).

12. Do you think upper level managers understand how some computer security rules adversely affect productivity?

○ Yes, and they try to fix it

○ Yes, they know but they can't fix it

○ Yes, they know but don't care

○ Not sure, but suspect it's yes.

○ Not sure, but suspect it's no

○ No

○ Don't know

Other (please specify)

13. We’ve all been given rules about access security. Some may be easy to follow, others may be hard or seemingly impossible to follow (e.g., instructions are incomprehensible, requires information we don’t have). Of the current access security rules with which you are familiar, please indicate the percent you estimate people (Should total to 100%):

a) Don't comply: rules are extremely difficult or impossible to complete or follow

b) Not worth the effort: rules could be completed in theory but requires so much effort and/or so reduces productivity that they are routinely ignored or worked around.

c) Can comply, but people routinely don't

d) Can comply, and people routinely do.

14. If you wish, please give brief examples of the types of access rule compliance issues you were thinking about regarding the above question.

15. When do you think most personnel would find circumvention of the access rules is justified? (Check as many as applies.)

□ Critical task, e.g., saving a life, keeping the grid up

□ When the rules are so foolish that nothing else makes sense

□ Access associated with role(s) make no sense, e.g., members of the same team can’t see all of the information because only some have official access

□ When allocation of access is foolish, e.g., people hired before November have access but others with similar functions and responsibilities don’t

□ When everyone else is circumventing a specific rule

□ When people were officially taught to use a workaround

16. [Almost done, Thank you.] If you were able to change access rules to make work more efficient, but not endanger security, what recommendations might you suggest?

17. In general, thinking about computer use in your work, what is most frustrating about your job?

18. What useful computer-related practices or techniques would you teach a new colleague in the same role as yours to accomplish daily tasks?

19. Thank you very much. If you wish to add additional comments or suggestions, you may do so in the box below. Please remember not to indicate your name or the name of the organization where you may work.

A.2 Survey for Cybersecurity Professionals

The survey for cybersecurity professionals begins on the next page.

Anonymous Survey about Computer Access, Worker's Understanding and Complian...

The purpose of the study: To understand how workers perceive computer access rules and their motivations to engage in workarounds to gain access to computer systems or parts of systems to which they are not supposed to access. We are not talking about hackers, rather we ask about barriers or inconveniences confronting personnel who seek to do their assigned work but are sometimes denied access because of problems such as lost passwords, required password changes, forgetting a specific log-on name, altered rules, system breakdowns, need to access the system via a different computer than usually used, etc. It is not a study of those with malicious intent.

Your participation in this research study is voluntary. If you decide not to participate, you are free to stop at any time. Withdrawal will not interfere with your work or with your organization. If you have questions about your participation or rights in this research, you can discuss them with the study investigator or members of the study team. You may contact Prof. Ross Koppel, Ph.D. at the University of Pennsylvania at: rkoppel@sas.upenn.edu.

1. Which “industrial” sector best describes the principal business area of your organization? (Note that we do not ask for the name of your organization or any identifying information.) You may check more than one category.

□ Agriculture, Forestry, Fishing and Hunting

□ Mining, Quarrying, and Oil and Gas Extraction

□ Utilities (electricity, water, waste treatment, etc.)

□ Construction

□ Manufacturing

□ Wholesale Trade

□ Retail Trade

□ Transportation and Warehousing

□ Information Technology

□ Finance and Insurance

□ Real Estate and Rental and Leasing

□ Professional, Scientific, and Technical Consulting Services

□ Management of Companies and Enterprises

□ Administrative & Support & Waste Management & Remediation Services

□ Educational Services

□ Health Care and Social Assistance

□ Arts, Entertainment, and Recreation

2. How would you define your role at your organization (may check more than one box, but indicate if that is your primary role):

	Yes, Primary	Yes, Secondary
I direct my organization's Information Technology services	○	○
I work on the help desk in the IT Dept. of my organization	○	○
I'm part of the IT team that addresses requests for modifications/fixes	○	○
I write or maintain software or hardware here	○	○
I train staff on IT subjects	○	○
I help set computer security policy for my organization	○	○
I work in an administrative role in the IT Dept (e.g., office manager).	○	○

Other (please specify)

3. Who sets policy about access to the computers and systems (e.g., desktops, network, laptops, servers) workers use most often in the course of their work?

□ No idea

□ Individual workplace unit (e.g., my dept or my boss)

□ Senior security or IT staff - Set at organization-wide level

□ Regulatory rules (rules set by regulators)

□ Professional or industry rules (e.g., all engineers will password protect…)

Other (please specify)

4. To the best of your knowledge, are your organization's policies on computer access based on: 1) systematic analysis of use patterns, 2) local rules, 3) set by others, 4) use data to help formulate that policy, and/or we use rules set by others (Executive Management, Political rules, Abstract rules…)

○ Don't know

○ We set policy based on our best judgement

○ Yes, users are told by policy makers that we use data to formulate policy

○ No, policy makers set rules based on other criteria

5. Do those who set security policy on access ask for input from users?

○ Yes

○ No

○ Don't know

Comment

6. If "Yes" to above: To the best of your knowledge, was their input considered?

○ Yes

○ No

○ Don't know

Comment

7. Many workers are frustrated by access policies that seem to provide little if any security benefit, and are also non-responsive to the needs of users who are trying to do their jobs. On a scale from 1 to 5, where 1 = “Not frustrated, policy appears to be reasonable” to 5 = “Very frustrated, policy seems arbitrary or not responsive to workflow needs,” please indicate your assessment of workers' views (may not be a correct reflection of the actual policy, but nevertheless, it's what most believe):

1 (Not Frustrated)	2	3	4	5 (Very Frustrated)
○	○	○	○	○

8. Even if you are frustrated by the access policy, do you see it as necessary to protect security, or do you see it as not well thought out, where the security benefit is less than the effort required to comply.

1 (Thoughtfully developed)	2	3	4	5 (More of a hindrance than anything else)
○	○	○	○	○

9. If people have a theory or belief about why the access rules may appear non-responsive to workflow needs, is it (can indicate multiple reasons):

	Very Likely	Likely	Un-likely	Don’t know	NA. Rules responsive
Not an issue; most perceive security policy as reasonable and the motivations as reasonable	○	○	○	○	○
Perceived incompetence of those who are in charge of security	○	○	○	○	○
Perceived arrogance of those who are in charge of security (“I know what is best for you – don’t question my authority…”)	○	○	○	○	○
Externally-imposed regulations which do not appear to be reasonable, dictating access rules	○	○	○	○	○
Using security as an excuse for laziness, e.g., they should fix something but just say it must be as is because of “security”	○	○	○	○	○

Other (please specify)

10. In general, please indicate how these various access rules (see below) are perceived by MOST people in your organization. (If appropriate, for each access rule select one of the button options. Otherwise, please write an explanation in the "It's Complicated" box)

	Generally sensible	Some-times sensible	Not sensible	Don’t know
Log-on rules	○	○	○	○
It’s complicated, Please explain…				
Need to use different passwords for different applications	○	○	○	○
It’s complicated, Please explain…				
Passwords—Complexity	○	○	○	○
It’s complicated, Please explain…				
Passwords change frequency	○	○	○	○
It’s complicated, Please explain…				
Access granting practices used by management	○	○	○	○
It’s complicated, Please explain…				
Inactivity- timing out rules	○	○	○	○
It’s complicated, Please explain…				
Systems with different access rules	○	○	○	○
It’s complicated, Please explain…				
Who gets access & why	○	○	○	○
It’s complicated, Please explain…				

11. Now, please briefly tell us of unwanted outcomes you may have heard about because of restricted access to legitimate users:

12. Do you think MOST workers believe that upper level managers understand how some computer security rules adversely affect productivity?

○ Yes

○ No

○ Don’t know

○ They know but don’t care

Other (please specify)

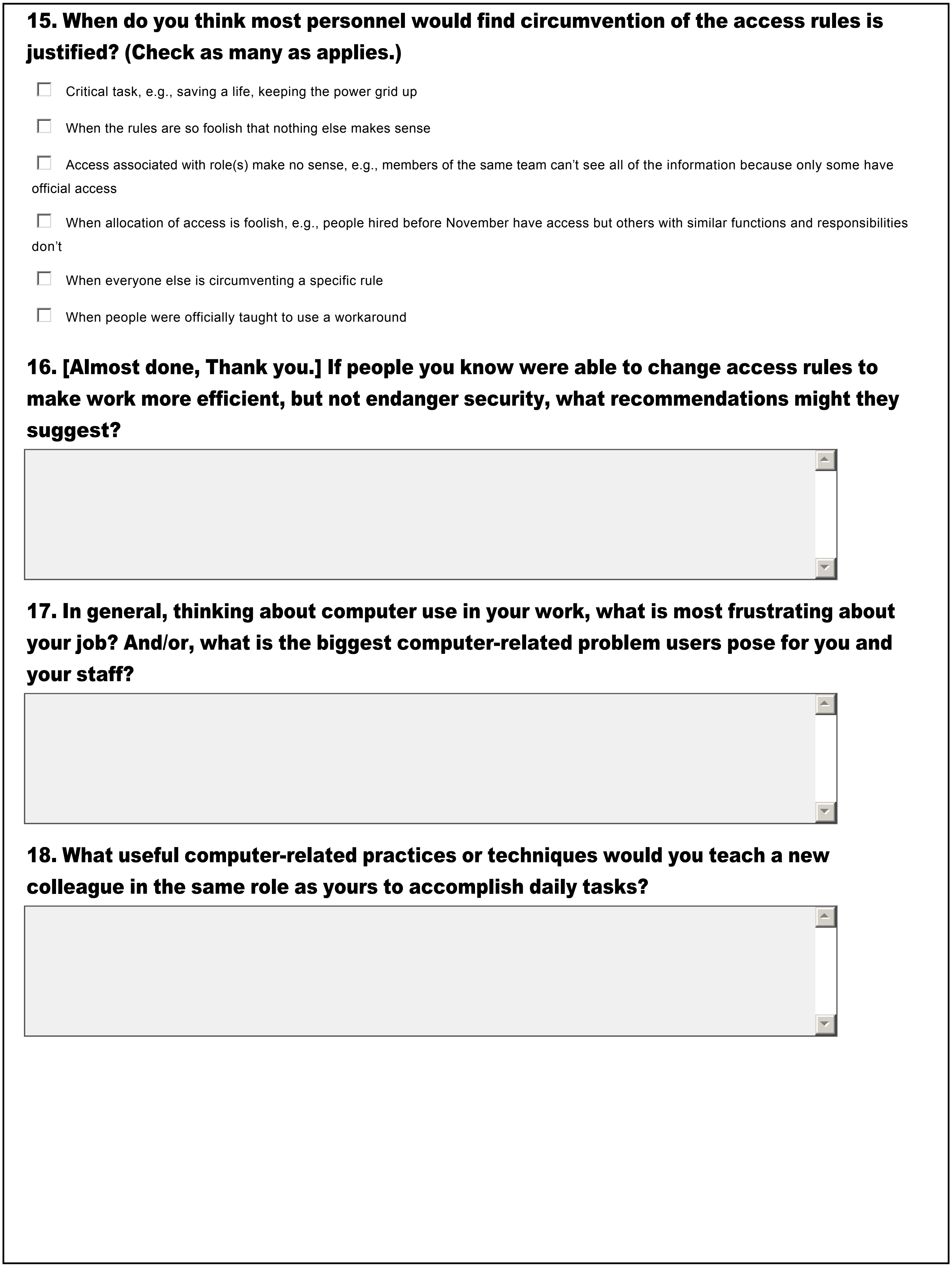
13. We’ve all been given rules about access security. Some may be easy to enact, others may be hard or seemingly impossible to enact (e.g., instructions incomprehensible, requires information we don’t have). Of the recent access security rules with which you are familiar, please indicate the percent you estimate people..... (Should total to 100%):

a) Can’t comply: rules that are extremely difficult or impossible to complete or follow

b) Too hard to comply: rules could be completed in theory but requires so much effort and/or reduces productivity that is not commensurate with security benefit that the rule were intended to provide

c) Can comply, and people routinely enacted these rules

14. If you wish, please give brief examples of the types of access rule compliance issues you were thinking about regarding this question (above).



15. When do you think most personnel would find circumvention of the access rules is justified? (Check as many as applies.)

□ Critical task, e.g., saving a life, keeping the power grid up

□ When the rules are so foolish that nothing else makes sense

□ Access associated with role(s) make no sense, e.g., members of the same team can’t see all of the information because only some have official access

□ When allocation of access is foolish, e.g., people hired before November have access but others with similar functions and responsibilities don’t

□ When everyone else is circumventing a specific rule

□ When people were officially taught to use a workaround

16. [Almost done, Thank you.] If people you know were able to change access rules to make work more efficient, but not endanger security, what recommendations might they suggest?

17. In general, thinking about computer use in your work, what is most frustrating about your job? And/or, what is the biggest computer-related problem users pose for you and your staff?

18. What useful computer-related practices or techniques would you teach a new colleague in the same role as yours to accomplish daily tasks?

19. Thank you very much. If you wish to add additional comments or suggestions, you may do so in the box below. Please remember not to indicate your name or the name of the organization where you may work.