

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

Dept. of Computer Science
Dartmouth College

vijayk@cs.dartmouth.edu

Sean Smith

Dept. of Computer Science
Dartmouth College

sws@cs.dartmouth.edu

Differential Perceptions



Security Person



User

SHUCS: <http://shucs.org>

(Science of Human Circumvention of Security)

Motivating Questions

- How are policies formed?
- Are policies sensible?
- Are they frustrating?
- Do users circumvent them? Is it justifiable?

Methodology

- Surveys administered via Survey Monkey
 - 15 cybersecurity professionals
 - 13 general users
 - 19 questions each

Policy Creation

- Who sets policies?
- What's the basis for policies?
- Is user input solicited when setting policies?

How Frustrated are You by 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

How Frustrated are You by Access Policies?

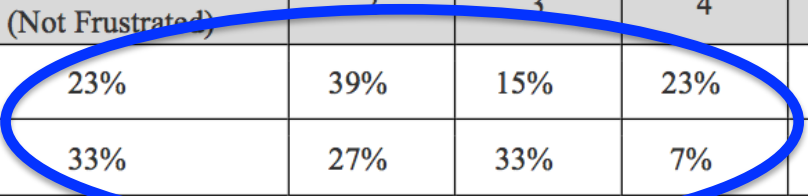
	1 (Not Frustrated)	2	3	4	5 (Very Frustrated)
General users	23%	39%	15%	23%	0
Cybersecurity professionals	33%	27%	33%	7%	0

How Frustrated are You by 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

How Frustrated are You by 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

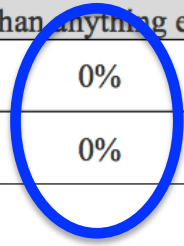


How Well Thought Out is the Policy?

	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%

How Well Thought Out is the 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%

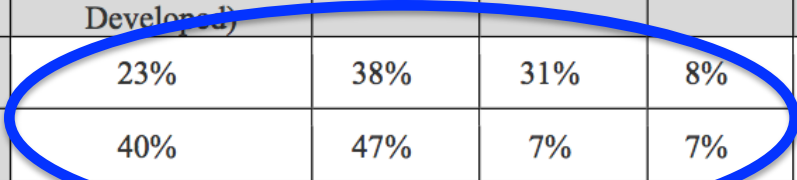


How Well Thought Out is the Policy?

	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%

How Well Thought Out is the 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%



How Well Thought Out is the 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%

1.83

2.24



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

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

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

When is Circumvention Justified?

	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%

Why are Access Rules (Perceived as) 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					

Why are Access Rules (Perceived as) 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					

Why are Access Rules (Perceived as) Foolish?

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

	Very Likely		Likely		Unlikely		Don't know		NA: Responsive Rules:	
	Gen	Pros	Gen	Pros	Gen	Pros	Gen	Pros	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										

Why are Access Rules (Perceived as) 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					

Examples of Compliance Issues



Cybersecurity Professionals

“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”

“Users write down certain passwords, because they are impossible to remember (they are set by the system rather than [by] users)”

General Users



“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.”

“Password and account sharing.”

“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’”

Discussion

- Limitations
 - Small sample size
 - Potential overlap b/w group demographics
- Findings
 - Security policies frustrate everyone!
 - Both groups recognize need for circumvention
 - Some differential perceptions
 - Pros responded “don’t know” more often.

Future Work

- Administer survey on broader scale.
- Given results, we can:
 - Inform security folks and users
 - Build more reliable models
 - Better allocate security resources



Thank you!



Our broader project: <http://shucs.org>

Questions? Suggestions? Comments?

Contact Information:

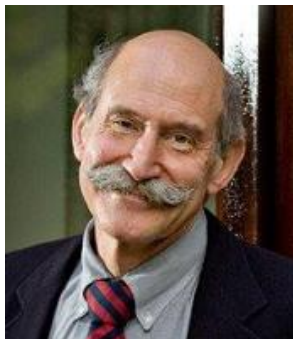
Ross Koppel: rkoppel@sas.upenn.edu

Jim Blythe: blythe@isi.edu

Vijay Kothari: vijayk@cs.dartmouth.edu

Sean Smith: sws@cs.dartmouth.edu

Ross
Koppel



Jim
Blythe



Sean
Smith

