What 4,500+ People Can Tell You – Employees' Attitudes Toward Organizational Password Policy Do Matter

Yee-Yin Choong(✉) and Mary Theofanos

National Institute of Standards and Technology, 100 Bureau Drive,
Gaithersburg, MD 20899, USA
{yee-yin.choong,mary.theofanos}@nist.gov

Abstract. Organizations establish policies on how employees should generate, maintain, and use passwords to authenticate and gain access to the organization's information systems. This paper focuses on employees' attitudes towards organizational password policies and examines the impacts on their work-related password activities that have security implications. We conducted a large-scale survey (4,573 respondents) to investigate the relationships between the organizational password policies and employees' password behaviors. The key finding of this study is that employees' attitudes toward the rationale behind cybersecurity policies are statistically significant with their password behaviors and experiences. Positive attitudes are related to more secure behaviors such as choosing stronger passwords and writing down passwords less often, less frustration with authentication procedures, and better understanding and respecting the significance to protect passwords and system security. We propose future research to promote positive employees' attitudes toward organizational security policy that could facilitate the balance between security and usability.

Keywords: Password behavior · Organizational password policy · Cybersecurity · Perception · Attitudes · Usability

1 Introduction

Passwords are the most widely used authentication mechanism for controlling employees' access to organizational information systems within public (e.g., government) and private sectors (e.g., corporations). To protect data integrity and system security, organizations often establish enterprise-specific password policies dictating how employees should manage their organizational passwords, including: password composition requirements on length and character usage, password expiration, password reuse policy (e.g., unique password for each system, can't reuse the past 10 same/similar passwords), and password storage requirements (e.g. can't write down, can't share with others). Those password policies are intended to ensure good password behaviors from the employees.

Often times, the stringent nature of those organizational password policies imposes humanly-impossible challenges for employees to be fully compliant, especially with

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 299–310, 2015.
DOI: 10.1007/978-3-319-20376-8_27

multiple passwords as there are fundamental limitations on human cognition, e.g., difficulty in generating complex passwords, limited memory span, memory decay, recognition vs. recall, and memory interferences [e.g., 1–4]. However, policy makers may not be fully informed of how many passwords an average employee must use to access their organization's information systems on a daily basis and how this could lead to errors and affect productivity. Policy makers may not be aware that the overly complex password policies only make it more difficult for employees to follow the directives. These demands on managing multiple passwords often impose high cognitive load on users and may indirectly weaken overall security as users are forced to act in insecure manners with respect to their passwords such as reusing password across multiple accounts, e.g., [3, 5, 6] or writing down passwords, e.g., [7, 8].

Research in the security and usability community in the past has provided invaluable insight on users' password behaviors. However, most of those studies are on non-work related accounts such as personal emails, websites, social media or school accounts. Questions regarding security activities and practices in the workplace such as employees' attitudes toward strict password policies, amount of time and effort employees spend on generating passwords, employees' authentication experiences and activities, and potential relationships among those questions have remained unanswered.

Research has shown that attitudes can guide, influence, shape, or predict behaviors as summarized by Kraus [9]. Employees' positivity is associated with positive attitudes and behaviors and may combat negative reactions to organization-wise changes or policy viewed as unfavorable [10]. In this study, we focus on investigating employees' password behaviors across three stages in the end-user password management lifecycle, namely, generation, maintenance, and authentication [11]. We examine employees' attitudes and experiences with respect to organizational policies in order to inform the development of effective password policies that take both security and usability into considerations. This research explores the relationships between the organizational password policy and employees' password and security activities to answer questions such as: are there possible associations amongst employees' attitudes toward password requirements of length and complexity and employees' password generation strategies or employees' propensity to store and "write down" passwords or how much employees experience login problems?

2 Methodology

We designed an on-line survey to collect data on employees' password management behaviors and their attitudes toward computer security and policy with respect to their work accounts and not personal or social accounts by sampling the United States (US) government workers. This paper focuses on the data collected from employees of the Bureaus of the US Department of Commerce (DOC). The survey was sent out via email to DOC employees asking for voluntary participation. The employees were informed that their responses would be collected anonymously to reduce possible social desirability bias and to encourage more honest responses [12].

The survey consists of nineteen questions related to password management and computer security and six demographic questions. The complete survey and detail results are documented in the NIST internal report – NISTIR7991 [13]. On average, it took those who elected to take the survey about fifteen minutes to complete. A total of 4,573 DOC employees completed the survey.

3 Results and Discussion

3.1 Attitudes Toward Password Policy and Requirements

In general, employees thought that their bureaus have clearly communicated the password policy (*very clear* – 53.8 %, *somewhat clear* – 33.1 %). Although "using the same password for different accounts" is prohibited in most bureaus' policies, more than 50 % respondents admitted that they have done that (*always* – 17.9 %, *more than half of my accounts* – 19.8 %, *about half of my accounts* – 18.9 %).

The majority of employees viewed the organizational password requirements as *burdensome*: *too long* (56.9 %) and *too complex* (50.7 %), as shown in Table 1. While most bureaus require password lifespan be shorter than 90 days, employees felt that their work-related passwords change too frequently as over 70 % of the respondents preferred that a password stays valid for longer than 90.

Table 1. Employees' attitudes toward password requirements

Question	Scale	Count	%
Password length requirement	Too long	2604	56.9 %
	About right	1644	36.0 %
	Too short	41	0.9 %
	No opinion	285	6.2 %
Password complexity requirement	Too complex	2318	50.7 %
	About right	2017	44.1 %
	Too simple	25	0.6 %
	No opinion	213	4.6 %
Preferred password lifespan	30 days or less	61	1.3 %
	31-60 days	263	5.8 %
	61-90 days	857	18.7 %
	91-120 days	831	18.2 %
	121-180 days	792	17.3 %
	181 days or more	1602	35.0 %
	No opinion	167	3.7 %

Although the bureaus have done a good job in communicating the password policies to their employees, these policies undermine employees' main concerns to be productive at their jobs. It results in usability issues and behaviors that may decrease security. The organizational password requirements have become more and more stringent over the past decade, i.e., long passwords, complex composition rules, and frequent change cycles, and have imposed burdens on the end-users. Many respondents expressed their frustration toward the requirements. One stated, "*Sometimes it's[sic] taken me 20 min to change a password to one that meets the requirements and isn't too far off from my other ones (so I can remember it!).*" Another one stated, "*I understand that for 'security' reasons it is good to change a password - but seriously are we all expected to magically remember 12 different passwords, most of which are 10 charecters[sic] long, and can't look like a word (I agree with the reason for the complexity - it just hard on the user).*" Yet another respondent echoed, "*The requirements have gotten so complex and the valid timeframe has shortened that that[sic] I often need to write down my passwords.*" Some respondent wrote, "*Security has become so complex, it's interfering with being able to do a job efficiently.*"

3.2 Importance of Employees' Attitudes Toward Password Requirements

While over 50 % of the respondents viewed the length and complexity requirements as *burdensome* (i.e. *too long*, *too complex*), there were still a good number of respondents who were quite receptive to those requirements (36 % chose *about right* for password length and 44 % chose *about right* for password complexity). It is of great interest to investigate whether these two divergent views hold any relationships to employees' password and security behaviors.

We categorize responses based on respondents' attitudes toward the password requirements: the *burdensome* group respondents view the length requirement as *too long* or view the complexity requirement as *too complex*; the *about right* group respondents view the length requirement as *about right* or view the complexity requirement as *about right*. We compare differences in responses from this categorization to examine their relationships with the employees' attitudes. Before performing any statistical analyses, we carefully examined the demographic characteristics of the respondents based on these divergent views to make sure that the demographic distributions are relatively consistent and comparable (see *Appendix*). As those survey responses are either nominal or ordinal data, we used a nonparametric statistical method, namely, Mann-Whitney Independent Samples U test, for comparisons between independent samples. The level of all tests for statistical significance is set to 0.05. It should be noted that any significant differences only show the existence of relationships between attitudes and users' security behaviors and experiences and do not provide the direction of causality.

3.2.1 Password Generation Considerations

The two most important considerations for the DOC respondents while generating passwords are *Easy to remember* (81.0 %) and *Compliant* (58.3 %), and the least is *Strong* (31.3 %) [12]. We investigate whether there are differences in those considerations between the *burdensome* group and the *about right* group, for employees' attitudes toward password length requirement and complexity requirement. All comparisons are statistically significant ($p < 0.05$).

To demonstrate those differences, we examine the responses of "*very important*" on those password generation considerations. We plot the data from those three considerations against the two divergent views toward the length and complexity requirements (Fig. 1) for the frequently used passwords. The trends for the occasionally used passwords are similar.

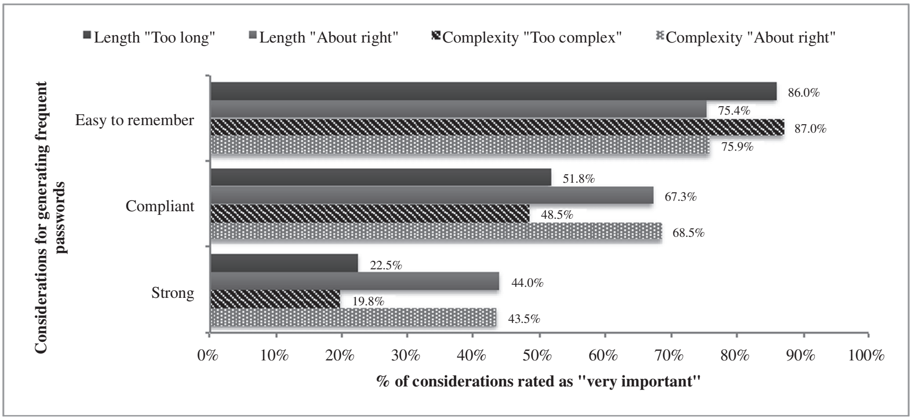

Fig. 1. Password generation considerations with respect to attitudes toward requirements

While *Easy to remember* is still the most important consideration during password generation for both groups, significantly more respondents who find the password requirements *burdensome* rate it as "*very important*" compared to those who find the requirements *about right*. For example, for the length requirement, 86.0 % of the *burdensome* group view *Easy to remember* as a very important password generation consideration while 75.4 % of the *about right* group rate it as very important. The attitudes toward the complexity requirement follow the same trend for the *Easy to remember* consideration with 11 % difference between the two groups.

Interestingly, it is the opposite for *Compliant* and *Strong* considerations. The difference between the *burdensome* respondents and the *about right* respondents is about 15 % for consideration of being *Compliant* for frequently used passwords, i.e. significantly more respondents who find the requirements *about right* rate *Compliant* as "*very important*"; whereas for *Strong* consideration, the percentage of the *burdensome* respondents rate *Strong* as "*very important*" is much lower (about half) than the percentage of the *about right* respondents.

3.2.2 Password Generation Strategies

Reusing passwords and modifying from existing passwords are often viewed as insecure user practices, e.g., [14, 15]. However, the top three password strategies used for generating frequently used passwords are: *Minor change* (67.8 %), *Existing password* (43.5 %), and *Recycle old passwords* (38.2 %) [12]. This indicates that employees are trying to minimize their effort in generating passwords by utilizing characters from existing passwords partially or fully, or they have difficulties in generating a completely different new password each time when a password generation event is triggered (e.g., old password expired, new account setup, password compromised).

When comparing between the *burdensome* group and the *about right* group, there are significant differences on all comparisons of those top three password generation strategies ($p < 0.05$). The *burdensome* group tend to use those strategies to generate their frequently used passwords more often compared to the *about right* group as shown in Fig. 2. The differences range from 7 % to 13 %.

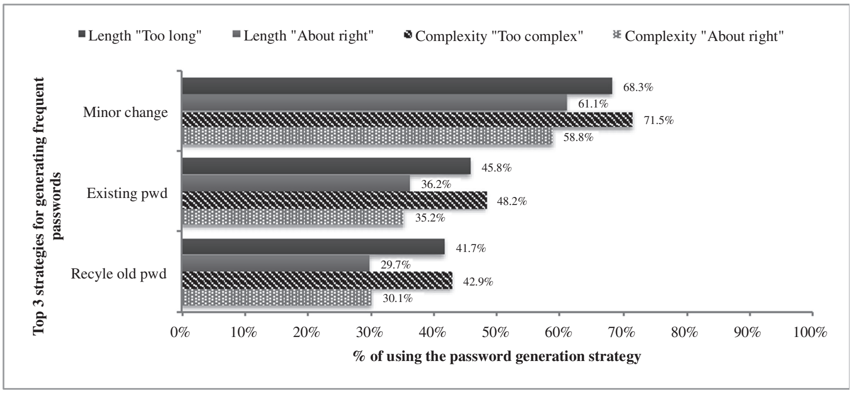

Fig. 2. Top 3 password generation strategies with respect to attitudes toward requirements

3.2.3 Storing or "Writing Down" Passwords

While it is a common practice in organizations to prohibit or discourage employees from storing their work-related passwords in any forms such as writing on paper or saving electronically in files or devices, it has been proven that solely relying on memorization is humanly impossible when users have to juggle multiple passwords at the same time. From this survey, the primary methods for tracking frequently used passwords are memorization (69.0 %), writing down on paper (64.4 %) (either disguised, locked, or in plain view), and saving electronically in files (28.8 %) (unencrypted or encrypted) [12]. However, if we look at various storing methods together (paper, file, electronic device, or password manager), a much higher percentage of the respondents (84.5 %) reported using at least one of those password storing methods for their frequently used passwords.

When we examine closely the relationship between employees' attitudes toward password requirements and their password tracking methods by comparing the two groups *burdensome* and *about right*, we find all comparisons statistically significant ($p < 0.05$). When employees think the passwords requirements are *burdensome*, they use memorization less, write on paper more, and store in files more, compared to respondents who think the requirements are *about right* (Fig. 3).

This phenomenon is even more pronounced when we examine the data further by looking at only the method of writing passwords on paper in plain view, e.g., on a sticky note next to a computer or on a desk. In Fig. 4, it shows that there is about a

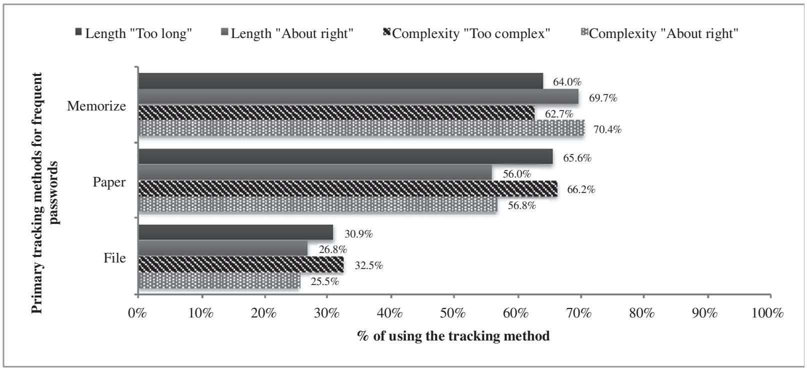

Fig. 3. Primary tracking methods with respect to attitude toward password requirements

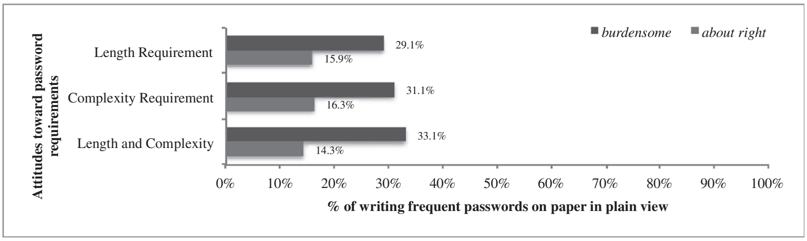

Fig. 4. Passwords on paper in plain view with respect to attitudes toward requirements

50 % drop of writing on paper in plain view when respondents think the requirements are *about right*, compared to *burdensome* respondents – from 29.1 % to 15.9 % regarding the length requirement and from 31.1 % to 16.3 % regarding the complexity requirement. When we further narrow it down to the two extreme cases, i.e., respondents who chose both *about right* and respondents who chose both *too long* and *too complex* on the requirements, the difference is even more – from 33.1 % to 14.3 %.

3.2.4 Experience with Login Problems

People reported the top three login problems experienced at work in the past six months as: mistyping password, forgetting password, and getting error messages while changing a password [12]. When respondents view the password requirements as *about right*, they are less likely to perceive *a lot* of frustration with the login problems. All comparisons for the top three login problems between the two groups *burdensome* and *about right* are statistically significant ($p < 0.05$).

To demonstrate those differences, we examine the responses of "*a lot*" of frustration on the top three login problems. It shows a significant finding that the percentage of the *burdensome* group experiencing a lot of login problems is about twice as much of the percentage of the *about right* group across all three login problems (Fig. 5). For example, there is about a 45 % drop of feeling frustrated with mistyping passwords when respondents think the requirements are *about right*, from the *burdensome* respondents – from 33.0 % to 18.4 % regarding the length requirement and from 34.4 % to 18.8 % regarding the complexity requirement.

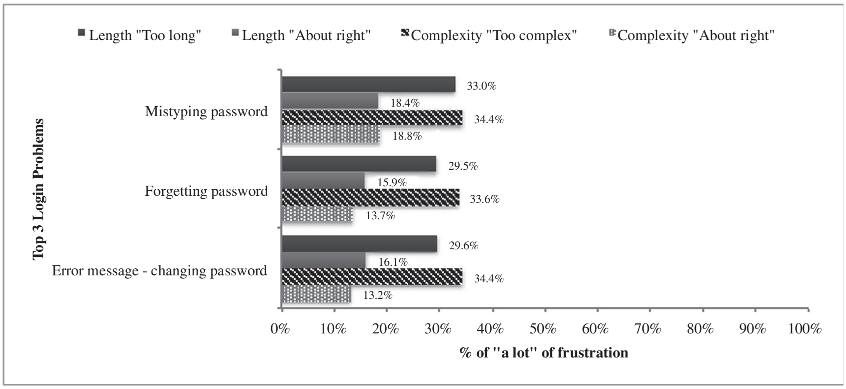

Fig. 5. Frustration with top 3 login problems with respect to attitudes toward requirements

3.2.5 Perception on Consequences of Compromised Passwords

We asked an open-ended question on people's perception of potential consequences if their work-related passwords were compromised. The majority of the free-form responses are related to the severity of the consequences, for example, "*None. My work is not sensitive.*" (classified as *None*), "*Minor consequences. Most data backed up in multiple ways.*" (classified as *Minor*), or "*Major, system compromise, violation of government trust.*" (classified as *Major*). We are surprised that a large percentage (35 % total: 6.8 % – *Don't know*, 22.8 % – *None*, and 5.3 % – *Minor*) of the responses did not perceive major consequences (only 9.9 % mentioned *Major* consequences) from potential compromises of the work-related passwords [12]. About 11 % of the responses mentioned that the consequences would depend on the sensitivity of the accounts compromised.

Upon further examination of the data, we discover an important relationship between the perceived severity of consequences from compromised passwords and the employees' attitudes toward the password requirements as shown in Fig. 6. While the perception of *Minor* consequences and *Don't know* are about the same across different groups, it is clear that the *about right* respondents are much less likely to answer *None* consequences (-14 % difference for length requirement, and -17.4 % difference for complexity requirement, both comparisons are statistically significant, $p < 0.05$) and they are more likely to perceive *Major* consequences (+7.1 % difference for length requirement, and +7.8 % difference for complexity requirement, both comparisons are statistically significant, $p < 0.05$) if their work-related passwords were compromised.

Another interesting finding is that the *about right* group is more likely to gauge the consequences depending on the types of accounts that the passwords might be compromised (+6.7 % for length requirement, and +6.6 % for complexity requirement, both comparisons are statistically significant $p < 0.05$).

Further analysis of the two extreme cases: respondents choosing both *about right* for the length and complexity requirements and respondents stating both as too *burdensome*, i.e. "too long" and "too complex," we find the same trends with even bigger differences (Fig. 6). For example, the both *about right* group is 21.3 % less likely to perceive *None* consequences, 10.5 % more likely to perceive *Major* consequences, and 8.1 % more likely to gauge consequences depending on accounts.

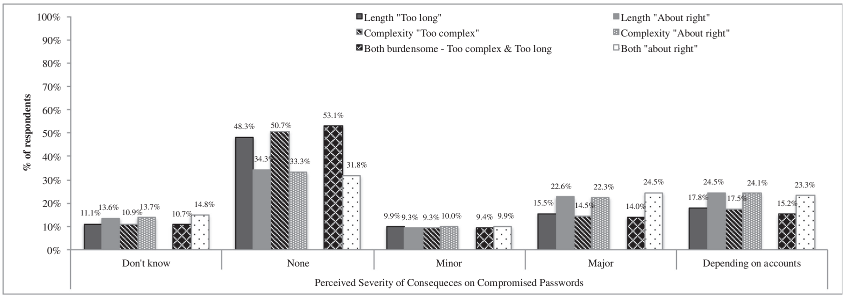

Fig. 6. Perceived severity of consequences with respect to attitudes toward requirements

4 Conclusions

The findings of this study on how people manage their work-related passwords show that the cognitive demands to comply with organizational password policies (e.g. length, composition rules, change frequency, reuse policy) and to maintain multiple passwords have pushed to the limits of human cognition. The DOC employees felt that the organizational policies require too long and too complex passwords, and the passwords have to be changed too often. As a result, in order to perform their jobs effectively, they have to employ coping mechanisms such as generating *easy to remember*, less *strong* passwords, reusing existing passwords, and "*writing down*" their passwords.

The key finding of this study is that employees' attitudes toward the rationale behind cybersecurity policies are statistically significant with their behaviors and experiences. When employees hold positive attitudes toward the password requirements, they tend to employ more secure behaviors and have more positive experiences throughout the three stages in password management lifecycle.

Compared to employees with negative attitudes toward the password requirements, positive employees, when generating passwords, indicate that *easy to remember* is less important, and *compliant* and *strong* become more important considerations. And, positive employees tend to reuse passwords less often. When maintaining their work passwords, positive employees are more likely to memorize passwords and "w*rite down*" passwords less often. Employees with positive attitudes perceive less frustration with login procedures and have better understanding and respecting to the significance of the need to protect passwords and system security.

While this survey was conducted with US federal employees, the findings are applicable to all organizations with formal password policies and security procedures for employees in the workplace. Currently, the security community is working toward long-term solutions for the password challenges, e.g., [16]. We will continue to perform research on the factors in promoting positive employees' attitudes toward cybersecurity in general and passwords in particular. It is also of great interest to investigate the direction of causality, i.e., if it's the positive attitudes that lead to better behaviors and experiences, or if it's the better behaviors and experiences that form the positive attitudes. We need to understand users' cognitive processes during the three stages of the password management lifecycle. It is imperative to research how people manage both work-related passwords and personal passwords in order to understand the interactions and the implications. Finally, organizational policies may need to be updated and training may need to be re-examined for its effectiveness.

Appendix: Demographic Distributions Grouped by Respondents' Attitudes Toward Password Requirements

Demographics		Attitudes toward length requirement		Attitudes toward complexity requirement	
		About right	Too long	About right	Too complex
Age	<= 25	4.5 %	2.9 %	3.6 %	3.5 %
	26–35	21.2 %	20.2 %	20.2 %	20.9 %
	36–45	22.6 %	23.2 %	22.4 %	23.4 %
	46–55	28.2 %	31.1 %	30.0 %	29.8 %
	56–65	19.2 %	17.9 %	19.1 %	18.3 %
	>= 66	2.6 %	2.2 %	2.9 %	1.8 %
	(not specified)	1.6 %	2.4 %	1.8 %	2.3 %
Gender	Male	57.6 %	57.8 %	57.4 %	58.0 %
	Female	39.1 %	38.8 %	39.6 %	38.4 %
	(not specified)	3.3 %	3.4 %	3.0 %	3.7 %
Education	High school	8.8 %	5.8 %	8.7 %	5.5 %
	Associate	5.2 %	5.3 %	5.4 %	5.0 %
	Bachelor	35.4 %	34.6 %	34.1 %	35.6 %
	Master	32.8 %	31.1 %	32.3 %	31.4 %
	Doctorate	12.8 %	16.9 %	14.6 %	15.9 %
	Professional degree	2.2 %	2.8 %	1.9 %	3.1 %
	(not specified)	2.8 %	3.6 %	3.1 %	3.4 %

(*Continued*)

(*Continued*)

Demographics		Attitudes toward length requirement		Attitudes toward complexity requirement	
		About right	Too long	About right	Too complex
Computer skill (self reported)	Novice	0.4 %	0.5 %	0.6 %	0.4 %
	Average	27.4 %	29.3 %	28.2 %	29.2 %
	Advanced	50.7 %	51.1 %	50.8 %	50.7 %
	Expert	21.1 %	18.7 %	20.1 %	19.2 %
	(not specified)	0.3 %	0.3 %	0.3 %	0.4 %
Federal service length (years)	< 1	6.1 %	5.3 %	6.5 %	4.7 %
	1–3	15.5 %	11.9 %	13.8 %	13.1 %
	4–5	7.8 %	7.9 %	7.9 %	7.7 %
	6–10	14.4 %	15.5 %	14.5 %	15.3 %
	11–14	11.5 %	11.1 %	10.2 %	12.1 %
	15–20	10.6 %	11.8 %	10.5 %	12.1 %
	> 20	33.7 %	35.9 %	36.1 %	34.5 %
	(not specified)	0.4 %	0.5 %	0.4 %	0.6 %
Job levels	Executive	1.6 %	2.1 %	1.5 %	2.2 %
	Manager	10.1 %	10.0 %	9.1 %	10.6 %
	Supervisor	13.1 %	14.1 %	12.5 %	15.0 %
	Team lead	10.9 %	12.1 %	10.9 %	12.1 %
	Non-supervisor	64.0 %	61.0 %	65.6 %	59.3 %
	(not specified)	0.3 %	0.8 %	0.4 %	0.8 %

References

1. Sasse, M.A., Brostoff, B., Weirich, D.: Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. BT Technol. J. **19**(3), 122–131 (2001)
2. Vu, K.P.L., Bhargav, A., Proctor, R.W.: Imposing password restrictions for multiple accounts: Impact on generation and recall of passwords. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting 47(11), 1331–1335 (2003)
3. Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K.: Generating and remembering passwords. Appl. Cogn. Psychol. **18**(6), 641–651 (2004)
4. Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B., Cook, J., Schultz, E.E.: Improving password security and memorability to protect personal and organizational information. Int. J. Hum Comput Stud. **65**, 744–757 (2007)
5. Florêncio, D., Herley, C.: A Large-Scale Study of Web Password Habits. In: Proceedings of the 16th International Conference on World Wide Web 2007, pp. 657–666 (2007)

6. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.: The tangled web of password reuse. In: Proceedings of NDSS (2014)
7. Inglesant, P.G., Sasse, M.A.: The true cost of unusable password policies: password use in the wild. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 383–392. ACM (2010)
8. Grawemeyer, B., Johnson, H.: Using and managing multiple passwords: a week to a view. Interact. Comput. **23**(3), 256–267 (2011)
9. Kraus, S.J.: Attitudes and the prediction of behavior: a meta-analysis of the empirical literature. Pers. Soc. Psychol. Bull. **21**(1), 58–75 (1995)
10. Avey, J.B., Wernsing, T.S., Luthans, F.: Can positive employees help positive organizational change? Impact of psychological capital and emotions on relevant attitudes and behaviors. J. Appl. Behav. Sci. **44**(1), 48–70 (2008)
11. Choong, Y.-Y.: A cognitive-behavioral framework of user password management lifecycle. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 127–137. Springer, Heidelberg (2014)
12. Ong, A.D., Weiss, D.J.: The impact of anonymity on responses to sensitive questions. J. Appl. Soc. Psychol. **30**(8), 1691–1708 (2000)
13. Choong, Y.-Y., Theofanos, M., Liu, H.-K.: United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study. NISTIR 7991, National Institute of Standards and Technology, Gaithersburg, US (2014)
14. Ives, B., Walsh, K.R., Schneider, H.: The domino effect of password reuse. Commun. ACM **47**(4), 75–78 (2004)
15. WEBROOT.com: New Webroot Survey Reveals Poor Password Practices that May Put Consumers' Identities At Risk (2010). http://www.webroot.com/us/en/company/press-room/releases/protect-your-computer-from-hackers. Accessed on 20 Jan 2015
16. National Strategy for Trusted Identities in Cyberspace. The White House, Washington, DC, US (2014). http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf. Accessed on 08 Jan 2015