Sharing or Non-sharing Credentials: A Study of What Motivates People to Be Malicious Insiders

Koichi Niihara[1(✉)], Michihiro Yamada[2], and Hiroaki Kikuchi[2]

[1] Meiji University Graduate School, Tokyo, Japan
niihara@meiji.ac.jp
[2] School of Interdisciplinary Mathematical Sciences, Meiji University, Tokyo, Japan

Abstract. The problem of an insider threat is a serious concern within organizations. It has been said that the weakest link in information security is the human element. Various causes of insider threats have been hypothesized. However, because there are so many potential causes of malicious insider threats, which factor has the greatest influence in inducing such threats remains unclear. In this paper, we focus on the most significant factor: *sharing credentials*. The objective of our study is to clarify the influence on the occurrence of malicious activities based on whether a credential is shared and whether a login ID is used. We conducted an experiment on a crowdsourcing service, Crowdworks, Inc., consisting of 198 participants to examine human behavior when attempting to perform malicious activities. Our results show that a non-indicated login ID has a statistically significant effect.

Keywords: Insider threat · Sharing credentials · Information breach

1 Introduction

Today, one of the biggest challenges faced by organizations is system misuse by insiders, and these actions can have a serious impact on organizations. It has been said that the weakest link in information security is the human element because insiders' behaviors rapidly change and are therefore difficult to predict. Insiders have the potential to cause serious damage to, and even threaten the existence of, an organization.

In order to detect malicious behaviors, many studies have been conducted from a human-computer interactive perspective [1–4]. Fagade and Tryfonas conducted a survey of IT professionals, managers and employees selected from a Nigerian bank and proposed ways in which information security could be embedded into security culture [5]. Classifying behaviors into two classes, positive and negative, Hausawi conducted interviews with security experts and identified a total of 21 negative and 15 positive security-related behaviors [6]. These survey-based studies are very useful for understanding insider behaviors and identifying possible features in relation to malicious activities. However, survey and interview responses are not always true, e.g., participants can pretend to be honest

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 353–365, 2017.
DOI: 10.1007/978-3-319-58460-7_25

and unintentionally protective of their organization. Moreover, it is not feasible to observe every step of a potential insider who intends to perform a malicious action.

To address the drawbacks of survey-based studies, we propose a new experiment-based study to explore key behaviors related to insider threats. Our study allows the risk posed to be quantified by arbitrary conditions. In the present study, we observed all actions made by a set of participants engaging in small pre-defined tasks from a website and counted the number of cheating behaviors they made that might be linked to insider threats.

Among 21 negative behaviors considered to be security concerns [6], we focus on the most significant: *sharing credentials*. For example, suppose a credential (e.g., an ID and password) is shared within a group to access a resource. The members of this group should be considered a more likely potential insider threat than a group whose members do not share such credentials.

It is impossible to observe the details of suspicious behavior, and it is difficult to conduct an experiment in an actual organization because of security policies. If participants are paid for their labor, they might not attempt to perform a malicious action. However, if participants are not paid enough, it is difficult to recruit an adequate sample.

To test our hypothesis, we conducted an experiment in which all participants in one group shared a single credential for logging in and working on a crowdsourcing service, Crowdworks, Inc., while participants in another group were each assigned individual credentials for the same task.

A total of 192 participants were included in the experiment. We compared differences in the number of malicious activities performed between the sharing and individual credential groups. Moreover, we examined the effects of using indicated (visible) vs. non-indicated (hidden) IDs for the website. We assumed that the group using non-indicated IDs would perform significantly fewer malicious activities than the group using non-indicated IDs.

The remainder of this paper is organized as follows. We describe the objectives of the paper and details of our experiments in Sect. 3. We summarize our results and give a discussion in Sect. 4. Our conclusions and plans for future works are presented in Sect. 5.

2 Related Works

For our related works, we consider studies regarding research on insider threats.

Cappli *et al*. classified insider threats into three sections: insider IT sabotage, insider theft of intellectual property, and insider fraud [7]. The present work deals with insider fraud.

Cohen and Felson [1] presented the 'routine activity theory', which argues that most crimes have three necessary conditions: a likely offender, a suitable target, and the absence of a capable guardian. Cressey [2] proposed the Fraud Triangle model to explain the factors present in every fraud situation: perceived

pressure, perceived opportunity, and rationalization. Greitzer *et al.* [3,4] provided some indicators of insider threats based on published case studies and discussions with experienced human resources professionals. According to these studies, various hypothesized causes of insider threats exist. However, because there are so many potential causes of malicious insider threats, which ones have the greatest effect on insider behavior remains unclear.

Cappli *et al.* proposed MERIT related to insider threats based on investigations of criminal records [8]. Nurse *et al.* proposed a framework for characterizing insider attacks [9]. Their models are convenient for administrators in solving the problems and analyzing the risks associated with insider threats. We demonstrated experimentally that placing participants in environments with low levels of surveillance is more likely to lead to insider threats [10]. Hausawi conducted an interview study to survey security experts about the behavior of end-users [6]. According to these studies, the most negative behavior is sharing credentials. However, how much sharing credentials increases the risk of insider threats remains unclear.

In this paper, we investigate the relationship between sharing credentials and the risk of malicious insider threats.

3 Experiment to Observe Malicious Activities

3.1 Objective

The objective of our study was to clarify the influence of sharing credentials on the performance of malicious activities. We also aimed to clarify the influence of using indicated IDs for working on a website.

3.2 Hypotheses

We make two hypotheses related to malicious activities. Let H_1, and H_2 be the hypothesized causes of insider threats of sharing credentials and using a non-indicated ID, defined as follows:

H_1 (sharing credentials) states that if an employee shares a common credential with others, then he/she will be a malicious insider.

H_2 (non-indicated ID) states that if an employee finds that no login ID is displayed on the website, then he/she will be a malicious insider.

3.3 Method

In order to test these hypotheses, we conducted an experiment for observing potential insider threats using a pseudo website as the environment. A total of 192 participants were recruited to use a crowdsourcing service, Crowdworks, Inc. They were then divided into four groups, A, B, C, and D, and assigned conditions, as defined in Table 1.

Table 1. Study groups and conditions.

Group	Credentials	Login ID	N
A	Sharing	Non-indicated	45
B	Individual		47
C	Sharing	Indicated	48
D	Individual		52

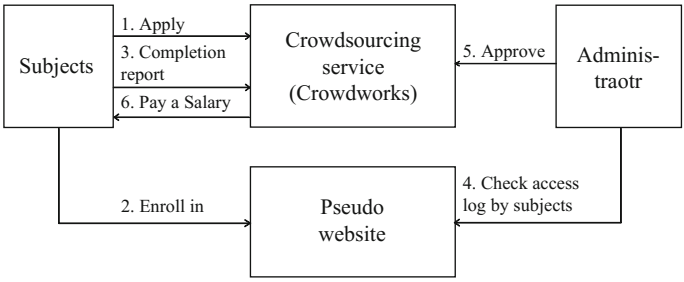

Fig. 1. Flow diagram of the experiment.

Figure 1 shows a flow diagram of the experiment. First, the participants answered a questionnaire composed of 14 items and performed data entry. When the participant finished his/her task, he/she would send a completion report. After we verified and approved the participant's access log, they were paid by the crowdsourcing service.

3.4 Participants

In our experiment, our target population was a set of employees in Japan. An employee subset was sampled from those who had completed the tasks in our experiment and were qualified users of the crowdsourcing service.

To improve the quality of the participants, we recruited only those who had submitted the necessary forms of identification to the company. The participants chosen from the crowdsourcing service were appropriate for our experiment because they had various attributes that were similar to normal employees.

3.5 Groups

In order to test H_1 (sharing credentials), the participants in groups A and C shared a common credential, such as a "guest" account, while those in groups B and D used individual credentials, such as user "93607".

In order to test H_2 (non-indicated ID), we did not indicate credentials to groups A or B, but we did to groups C and D.

In this way, we assigned a different malicious insider condition to participants in each group. We were interested in how many malicious activities would be observed in each group. In this experiment, we attempted to identify the primary causes of malicious activities by insiders.

3.6 Tasks

First, the participants confirmed the terms of use shown in the pseudo website. For details of the terms of service, see the Appendix A. Next, the participants answered a questionnaire composed of six questions, performed data entry, and then answered a questionnaire composed of seven questions. The participants entered text identical to that in two sample PDF documents written in Japanese and English. For details of the survey and the data entry jobs, see the Appendix B. Finally, the participants completed the tasks.

In order to observe the responses of participants who had trouble performing their tasks, we intentionally inserted a fault in the questionnaire in that the website would never accept the response to Question 6. Participants tried to resolve this issue in one of two ways:

- "edit" button prepared for an administrator (prohibited for participants)
- "help" button (correct response)

3.7 Obstacles

Malicious activities were not performed very frequently. Hence, we intentionally included some obstacles that would make participants choose whether to perform their tasks in a prohibited way.

Unacceptable Question 6. After the participants answered 13 questions and carried out data entry, they felt that they had completed all tasks. However, they would then receive the following warning message: 'You have not yet finished Question 6'. The reason for this error is that the system does not ask them Question 6.

To complete their task, the participants could deal with the problem in the following ways:

"Help" Page. If participants accessed the help page, they would be asked to answer 13 questions, after which, they would be regarded as having completed all tasks.

"Edit Button" for Question 6. If participants clicked the "edit" button for Question 6 in an attempt to modify it, this was labeled as a "malicious activity" because it was prohibited in the terms of use.

Synthesized Text of PDF Document. The pseudo business website gives synthesized text to participants who engage in data entry jobs.

For details of the text, see the Appendix B.2. The text looks like meaningless sentences that no one would want to read.

These are aimed at reducing the motivation of the participants and encouraging them to perform more malicious activities than usual.

3.8 Malicious Activities

Malicious activities were detected based on accurate logs that list what activities have been performed, at what time, and by whom. We defined the following malicious activities as prohibited actions:

(1) Violation
Gaining unauthorized access, e.g., clicking the administrator's edit button.
(2) Copy and paste
Performing unauthorized activities, e.g., pressing the Ctrl+C or Ctrl+V key.
(3) Sabotage
Inputting random or wrong text in the data entry website.
(4) Low score
Answering the questions randomly. To test whether the participants answered the questions honestly, we repeated the same questions twice in random order and then checked the consistency. We evaluated the consistency score S_i, which was defined as follows:
   (a) In the case of a single-response questionnaire, if the first answer is equal to the second, we add 10 points to S_i.
   (b) In the case of a multiple-response questionnaire, if two answers are consistent, we add 25 points to S_i. However, 5 points are deducted for each inconsistent answer.

   Five single-response and two multiple-response questionnaire were provided. The highest possible consistency score S_i was 100.

3.9 Methods of Detection

We used a php script to detect malicious activity. We used javascript to detect malicious behavior such as pressing the Ctrl+C or Ctrl+V key or copying and pasting by right-clicking. We manually analyzed the website log, all survey answers and all input text in the database. Table 2 shows the relationship between malicious activities and methods of detection.

Table 2. Relationship between malicious activities and methods of detection.

Malicious activities	Method of detection
(1) Violation	php script
(2) Copy and paste	javascript
(3) Sabotage	log analysis
(4) Low score	log analysis

4 Result

4.1 Demographic Characteristics of the Participants

Table 3 shows the demographic characteristics of the participants in each group, where N is the number of users in each group. Note that the numbers of participants in a group were not always identical, e.g., there were slightly fewer participants in group A than in group D. This was because we assigned participants to each group in turn, and some participants did not complete the task, resulting in uneven group sizes.

Table 3. Number of users.

Group		A	B	C	D	Total
Sex	Male	18	21	18	21	78
	Female	27	26	30	31	114
Age (years)	under 19	1	1	2	1	5
	20–29	13	14	9	12	48
	30–39	13	16	16	25	70
	40–49	11	12	19	10	52
	50–59	6	4	0	4	14
	60–69	1	0	2	0	3
Job	Office worker	10	16	8	18	52
	Proprietor	11	4	11	10	36
	Student	5	4	4	3	16
	Homemaker	9	7	13	8	37
	Part-time employee	4	9	7	6	26
	None	3	2	4	4	13
	Other	3	5	1	3	12
N		45	47	48	52	192

4.2 Number of Users Who Performed Malicious Activities

Table 4 shows the number of malicious users who performed malicious activities in our experiment. The number of users N is the sum of the two groups in the same category. For example, the number of users sharing credentials are the sum of A and C. In the sharing credentials group, 28 of 93 users copied and pasted text by right-clicking. Surprisingly, more users in the individual credentials group copied and pasted text compared with the sharing credentials group. Similarly, more participants using indicated IDs were found to be performing malicious activities compared with those using non-indicated IDs ($n = 27$). Remarkably, the low scores (4) of some of the malicious participants of increased when they shared credentials within a group.

Table 4. Number of users who performed malicious activities.

Group	N	(1) Violation	(2) Copy and paste	(3) Sabotage	(4) Low score
Sharing credentials (A+C)	93	14	28	6	20
Individual credentials (B+D)	99	18	35	4	13
Non-indicated ID (A+B)	92	18	27	3	21
Indicated ID (C+D)	100	14	36	7	12

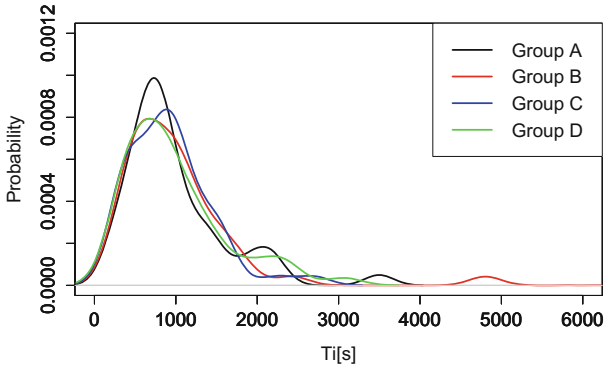

Fig. 2. Probability density function of elapsed time T_i for each group.

Figure 2 shows the probability density function of the elapsed time of the task T_i for each participant i. The elapsed time of task T_i is the difference between the starting and finishing times. A small difference was found between groups. Figure 3 shows the probability density function of the consistency score S_i for each group. Group A had the smallest average consistency.

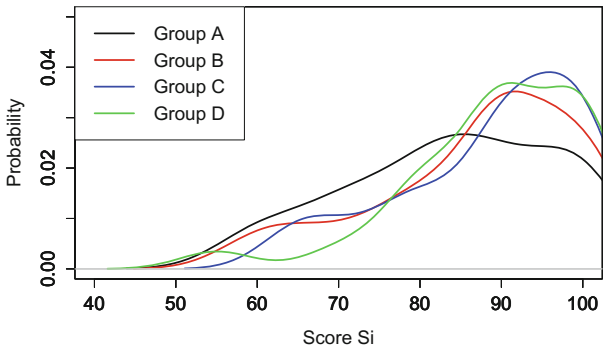

Fig. 3. Probability density function of score S_i for each group.

4.3 Chi-Square Test

To evaluate the confidence of our experimental results, we performed a chi-square test on the number of malicious activities for (1), (2), (3) and (4).

We had the following two hypotheses:

The null hypothesis (H_0): there is no correlation between the groups and malicious activity. Malicious activities are performed independent of the group condition.
The alternative hypothesis (H_1): there is a correlation between the hypothesized causes and malicious activity.

Table 5 shows the results of the chi-square test. The results show that low scores for malicious activities (4) were significantly more frequently observed when the website did not indicate a login ID. However, the P values for activities (1), (2) and (3) were too large to reject the null hypothesis. Therefore, we conclude that only (4), a low score, was dependent on whether IDs were indicated with 90% confidence.

4.4 Discussion

First, we consider the influence of non-indicated IDs on malicious behavior. Based on Table 5, a low score (4) for malicious activities depended on the non-indicated ID condition. If no login ID was shown on the website, more malicious activities were performed. We therefore conclude that people do not stay motivated to work when no login ID is indicated.

Second, we observed that too many malicious activities occurred in terms of clicking the edit button. As we explained in Sect. 3.7, Question 6 was designed to not be answerable in order to tempt potential malicious participants to click the "edit button". However, almost all participants clicked the "edit" button. We therefore believe that the participants clicked the button innocently without realizing that it was a prohibited activity. Alternatively, careless participants simply failed to notice this rule in the terms of use. Since it was useless to identify

Table 5. Chi-square test results

Hypotheses	Malicious activity	χ^2	*df*	P value
H_1 (Sharing credentials)	(1) Violation	0.1502	1	0.698
	(2) Copy and paste	0.3843	1	0.535
	(3) Sabotage	0.1819	1	0.669
	(4) Low score	1.8108	1	0.178
H_2 (Non-indicated ID)	(1) Violation	0.7054	1	0.401
	(2) Copy and paste	0.6837	1	0.408
	(3) Sabotage	0.7053	1	0.401
	(4) Low score	3.2217	1	0.073*

the hypothesized causes of malicious behavior, we excluded these activities in our analysis.

Finally, we remark on the relationship between individual and temporal credentials. In our experiment, we expected that users who were assigned individual credentials would perform fewer malicious activities. However, they might not have regard themselves as having individual credentials very seriously because they were only for one-time use. If we had assigned more permanent credentials, such as Social Security Numbers, the participants may have viewed them as being more serious.

5 Conclusions

In the present study, based on a survey of research related to insider threats, we focused on the occurrence of malicious activities under the condition of sharing or individual credentials. To clarify the effects, we conducted an experiment involving 198 participants who performed a small task to observe malicious activity. We observed significantly more malicious activity when a user ID was not indicated compared with when it was. However, unexpectedly, users who were sharing credentials did not perform more malicious activities than users who had individual credentials.

In future research, we plan to investigate the reasons underlying the differences seen in the number of malicious activities performed in accordance with the conditions of malicious insiders.

A Terms of Use

- Terms of use
  A record of your visit and attributes will only be used for research purposes. We do not identify the user, and we will only publish the processed data in a research paper. Appropriate safety control measures have been carried out for all information on this site.
- Things to note
  Please read the questionnaire carefully before answering the survey.
- Prohibited actions
  - In survey tasks
    * Clicking the “back” button
    * Visiting the website by directly specifying the URL
  - In data entry tasks
    * Copying and pasting by right-clicking or pressing the Ctrl+C or Ctrl+V key
  - In both tasks
    * Clicking the edit button intended for the administrator
- Inquiries
  If something is unclear or you experience trouble during the task, please access the inquiry page to contact the administrator.

B Contents of Tasks

B.1 Survey Tasks

- Question 1. How often do you eat curry and rice?
  A.1. 7 or more times per week. A.2. 5–6 times per week A.3. 3–4 times per week A.4. 1–2 times per week A.5. 2–3 times per month A.6. Once per month A.7. Less than once per month
- Question 2. What is your favorite type of curry and rice?
  A.1. Curry and rice cooked by your family A.2. Indian curry served in an Indian restaurant A.3. Curry and rice served in a Japanese curry restaurant A.4. Ready-to-eat curry A.5. Curry and rice served in a family or beef bowl restaurant
- Question 3. What is your favorite ingredient in curry and rice?
  A.1. Pork A.2. Chicken A.3. Beef A.4. Vegetables A.5. Seafood
- Question 4. What is your favorite ingredient related to fruits or vegetables in curry and rice?
  A.1. Potatoes A.2. Onions A.3. Cheese A.4. Apples A.5. Eggplant
- Question 5. How long do you continue eating leftover curry and rice made by your family?
  A.1. The same day only A.2. Until the next day A.3. Up to 3 days after A.4. Up to 5 days after A.5. Up to 7 days after A.6. More than a week after
- Question 6. What is the most important aspect of curry and rice?
  A.1. Spiciness A.2. Sweetness A.3. Fragrance A.4. Depth of flavor (Koku in Japanese) A.5. Deliciousness (Umami in Japanese)
- Question 7. How much do you spend on one curry and rice meal at a restaurant?
  A.1. Less than 500 yen A.2. 500–749 yen A.3. 750–999 yen A.4. 1,000–1,499 yen A.5. 1,500–1,999 yen A.6. 2,000–4,999 yen A.7. 5,000 yen or more

The following questions contain the same contents, but the order of the answers has been changed.

- Question 8. What is your favorite ingredient in curry and rice?
  A.1. Pork A.2. Beef A.3. Vegetables A.4. Chicken A.5. Seafood
- Question 9. What is your favorite ingredient related to fruits or vegetables in curry and rice?
  A.1. Onions A.2. Potatoes A.3. Eggplant A.4. Apples A.5. Cheese
- Question 10. What is the most important aspect of curry and rice?
  A.1. Fragrance A.2. Spiciness A.3. Depth of flavor (Koku in Japanese) A.4. Sweetness A.5. Deliciousness (Umami in Japanese)
- Question 11. How often do you eat curry and rice?
  A.1. Less than once per month A.2. Once per month A.3. 2–3 times per month A.4. 1–2 times per week A.5. 3–4 times per week A.6. 5–6 times per week A.7. 7 or more times per week

– Question 12. How much do you spend on one curry and rice meal at a restaurant?
  A.1. 5,000 yen or more A.2. 2,000–4,999 yen A.3. 1,500–1,999 yen A.4. 1,000–1,499 yen A.5. 750–999 yen A.6. 500–749 yen A.7. Less than 500 yen
– Question 13. What is your favorite type of curry and rice?
  A.1. Indian curry served in an Indian restaurant A.2. Curry and rice served in a Japanese curry restaurant A.3. Ready-to-eat curry A.4. Curry and rice served in a family or beef bowl restaurant A.5. Curry and rice cooked by your family
– Question 14. How long do you continue eating leftover curry and rice made by your family?
  A.1. More than a week after A.2. Up to 7 days after A.3. Up to 5 days after A.4. Up to 3 days after A.5. Until the next day A.6. The same day only

B.2 Data Entry Task

– Please input the following text.
  Saffron is put in a water 1/2 cup, and avails oneself and takes out the color for about 30 min. I sharpen rice, give it to a basket and drain off water for about 20 min. The seafood blanched beforehand is moved to the pot and it's boiled for about 15 min.

References

1. Cohen, L.E., Felson, M.: Social change and crime rate trends: a routine activity approach. Am. Sociol. Rev. **44**(4), 588–608 (1979)
2. Cressey, D.R.: Other People's Money: A Study in the Social Psychology of Embezzlement. Free Press, Glencoe (1953)
3. Greitzer, F.L., et al.: Identifying at-risk employees: modeling psychosocial precursors of potential insider threats. In: 2012 45th Hawaii International Conference on System Sciences, pp. 2392–2401 (2012)
4. Greitzer, F.L., Frincke, D.A.: Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. Insider Threats Cyber Secur. **49**, 85–113 (2010)
5. Fagade, T., Tryfonas, T.: Security by compliance? A study of insider threat implications for Nigerian banks. In: Tryfonas, T. (ed.) HAS 2016. LNCS, vol. 9750, pp. 128–139. Springer, Cham (2016). doi:10.1007/978-3-319-39381-0_12
6. Hausawi, Y.M.: Current trend of end-users' behaviors towards security mechanisms. In: Tryfonas, T. (ed.) HAS 2016. LNCS, vol. 9750, pp. 140–151. Springer, Cham (2016). doi:10.1007/978-3-319-39381-0_13
7. Cappelli, D., Moore, A., Trzeciak, R.: The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley Professional, Boston (2012)
8. Cappelli, D., et al.: Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System. Software Engineering Institute, Carnegie Mellon University (2008)

9. Nurse, J.R.C., et al.: Understanding insider threat: a framework for characterising attacks. In: 2014 IEEE Security and Privacy Workshops (SPW 2014), San Jose, CA, pp. 214–228 (2014)
10. Niihara, K., Kikuchi, H.: Primary factors of malicious insider in e-learning model. In: Stephanidis, C. (ed.) HCI 2016. CCIS, vol. 617, pp. 482–487. Springer, Cham (2016). doi:10.1007/978-3-319-40548-3_80