Primary Factors of Malicious Insider in E-learning Model

Koichi Niihara(✉) and Hiroaki Kikuchi

Graduate School, Meiji University, Tokyo 164-8525, Japan
{niihara,kikn}@meiji.ac.jp

Abstract. There have been recent incidents in which large amounts of personal information have been leaked by malicious insiders. Organizations are now required to prepare countermeasures to deal with insider threats. To identify the primary causes of malicious insider behavior, an experiment was conducted using a pseudo e-learning website. A total of 100 subjects were recruited by crowd-sourcing and divided into four groups with different hypothesized causes of insider threat. The number of malicious activities in each group was observed. The results show a correlation between the hypothesized causes of insider threat and malicious activities.

Keywords: E-learning · Insider threat · Crowd-sourcing · Information leakage

1 Introduction

In July 2014, an incident occurred [1] in which large amounts of personal information of about 29 million users were leaked by a malicious insider. Subsequently, organizations were required to prepare countermeasures to deal with insider threats. However, the primary causes of insider threats remain unclear because there are so many factors in malicious activities to be considered.

The objective of this research was to identify the primary causes of malicious activities. By identifying the underlying factors involved in malicious activities by insiders, organizations can more effectively tailor their efforts to reduce the risk of malicious insider threats.

However, it is not easy to observe malicious activities because they occur infrequently. Moreover, strict security policies prevent researchers from observing employees performing suspicious behaviors in real organizations.

To address the difficulties in observing malicious activities, we conducted an experiment using a pseudo e-learning website that provided an environment for setting various traps, which corresponded to specific causes of insider threats. Using the crowd-sourcing service, Lancers, Inc., we recruited 100 subjects for our experiment. The results show the correlation between the hypothesized causes of insider threat and malicious activities. The main finding of our study is that a low level of monitoring is the most significant cause of insider threat. An employee

C. Stephanidis (Ed.): HCII 2016 Posters, Part I, CCIS 617, pp. 482–487, 2016.
DOI: 10.1007/978-3-319-40548-3_80

who knows that he or she is not under surveillance is 17.9 times more likely to perform malicious activities than an employee kept under sufficient surveillance by the organization.

The 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. We provide conclusions and future works in Sect. 5.

2 Related Works

Cohen *et al.* [2] 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 *et al.* [3] proposed the Fraud Triangle model to explain the factors that are present in every situation of fraud: perceived pressure, perceived opportunity, and rationalization. Greitzer *et al.* [4,5] provided some indicators of insider threat based on published case studies and discussions with experienced human resources professionals. The Nikkoso Research Foundation for Safe Society [6] proposed some factors related to insider threat based on investigations of criminal records.

According to these studies, various hypothesized causes of insider threat exist. However, because there are so many potential causes of malicious insider threat, it is unclear which ones have the greatest effect on insider behavior.

3 Primary Factors of Malicious Insider in E-learning Model

3.1 Objective

Our research objective was to identify the primary causes of malicious insider behavior. By identifying these, organizations can focus their efforts on controlling them, minimizing both the cost of compliance and the risk of insider threat.

Based on a recent study [6] we proposed the following three hypotheses related to malicious activities: Let H_1, H_2, and H_3 be the hypothesized causes of insider threats of stress, violence, and low monitoring, defined as follows:

H_1 (stress) states that if an employee is feeling stressed then he/she will be a malicious insider.

H_2 (violence) states that if an employee is treated in a violent manner, he/she will be a malicious insider.

H_3 (low monitoring) states that if an employee finds that no one is keeping him/her under surveillance, he/she will be a malicious insider. An example is a workplace that neglects to monitor its employees.

3.2 Method

To explore the connection between the causes of malicious insider behavior and the malicious activities, we conducted an experiment using a pseudo e-learning website as the environment for observing potential insiders. Using the crowdsourcing service, Lancers, Inc., we recruited 100 subjects for our experiment. To ensure the quality of workers, we chose Lancers-certified workers with a history of at least 95 % approval rates.

We divided the sample of 100 into four groups, A, B, C, and D, and assigned each group a different malicious insider condition, as follows:

Group A To evaluate H_1, subjects in this group had only 20 min to complete the e-learning task, while subjects in the other groups had more time (average time of 25–45 min).

Group B To evaluate H_2, we gave subjects in this group a threatening warning message with a frightening picture.

Group C To evaluate H_3, we informed all groups except group C that all access and behaviors are logged on the site, and if illegal access was detected they would face a fine.

Group D To evaluate the effects of the insider threat factors in the first three groups, group D was used as a control.

3.3 Definition of Malicious Activities

We defined the following malicious activities as prohibited performances:

(1) Violating a rule of prescribed screen transition, e.g., pressing the back button.
(2) Answering without reading the material and progressing to the next page too quickly to have read the material, e.g., reading speed of 1000 words per 3 or 4 s.
(3) No answer as answering a test with no check.
(4) Reading HTML sources from the browser. This can be detected by fake answers written in source code.

3.4 Result

Table 1 shows the number of malicious activities for each group, where N is the number of users for each group.

Figure 1 shows reading speeds, S_i, with respect to the number of characters of i-th material, where the dashed line indicates the 95 % prediction interval of the regression equation of reading speed. Where reading speed S_i exceeded the dashed line, we determined that the subject performed the malicious activity of (2) (answering without reading).

Table 1. Number of users that caused malicious activities for each group

Malicious activities	group A	group B	group C	group D	Total
1 Breach of screen transition	6	4	9	9	28
2 Answer without reading	5	6	11	1	22
3 No answer	0	0	3	1	4
4 Reading HTML sources	0	0	1	0	1
N	24	22	27	27	100

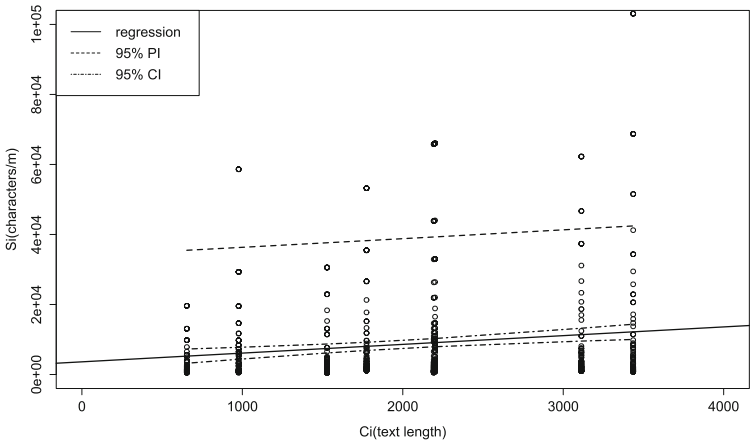

Fig. 1. Scatter plot between reading speed S_i and number of characters C_i

4 Evaluation

4.1 Chi-Square Tests

To measure the significance of our experimental results, we performed chi-square tests on the number of malicious activities of (1) and (2) for some hypothesized causes. We did not investigate malicious activities (3) or (4) further because there were only a few of these (4 cases and 1 case, respectively). In our test, we had:

The null hypothesis (H_0): there is no correlation between malicious activity and the hypothesized causes.
The alternative hypothesis (H_1): there is a correlation between malicious activity and the hypothesized causes.

Table 2 shows the chi-square test results. A statistically significant level of malicious activity (2) occurred when subjects were not monitored in their environment. However, activity (1) did not reach significance, and we were unable to reject the null hypothesis.

Table 2. Results of chi-square tests

Malicious activities	χ^2	*df*	P value
1 Breach of screen transition	1.921	3	0.589
2 Answering without reading	10.76	3	0.0131**

** significant at $P < 0.05$

4.2 Logistic Regression Analyses

Subjects have many attributes, such as age, sex, educational history, employment status and so on, that could have a large effect on our results. To identify the primary factors and discard the confounding factors, we performed logistic regression analyses.

In our logistic model, dependent variables of malicious activities were estimated based on independent variables of membership to groups (hypothesized causes of insider threat), defined as follows:

Let x_a, x_b, and x_c be coefficients, meaning membership to Group A, B, and C, respectively. The probability of being a malicious insider p is

$$p = \frac{1}{1 + \exp(3.258 - 1.923x_a - 2.277x_b - 2.883x_c)}, \tag{1}$$

where the logistic function (inverse function) is

$$\log \frac{p}{1-p} = -3.258 + 1.923x_a + 2.277x_b + 2.883x_c. \tag{2}$$

The odds ratios of groups A, B, and C are 6.84, 9.75, and 17.9, respectively.

Table 3 shows the results of the logistic regression analyses.

Table 3. Results of the logistic regression analyses

Variable	Estimate	Std. Error	Z value	P value
Intercept (D(No cause))	−3.258	1.019	−3.199	0.00138***
A (Stress)	1.923	1.136	1.693	0.09044*
B (Violence)	2.277	1.125	2.023	0.04304**
C (Low monitoring)	2.883	1.091	2.642	0.00824***

* significant at $P < 0.1$
** significant at $P < 0.05$
*** significant at $P < 0.01$

4.3 Discussion

Type (2) malicious activities for each group were significant. Malicious activity types (1), (3), and (4) were observed but the numbers for each group were

not statistically significant. Hypothesis H_3 was supported in our experiment: the risk of an insider threat for an employee who knows that he/she is not under surveillance is 17.9 times greater than that for employees who are under surveillance. Based on these results, we suggest that organizations should give more attention to further monitoring to reduce the risk of insider threats. Table 3 shows a statistically significant effect of employee performing malicious activities when a threatening alert was given (group B). H_2 is significant correlation in Table 3.

5 Conclusions

We studied the primary factors of malicious insider behavior by conducting an experiment using a pseudo e-learning website. Our statistical analysis shows a correlation between the lack of monitoring employee and malicious activities. Our future works will focus on methods of surveillance, with real-life testing, to determine why insiders sell personal information.

References

1. Benesse Holdings Inc: Report and response regarding leakage of customers' personal information (2014). http://blog.benesse.ne.jp/bh/en/ir_news/m/2014/09/10/uploads/news_20140910_en.pdf
2. Cohen, L.E., Felson, M.: Social change and crime rate trends: A routine activity approach. Am. Sociol. Rev. **44**(4), 588–608 (1979)
3. Cressey, D.R.: Other People's Money; A Study in the Social Psychology of Embezzlement. Free Press, Glencoe (1953)
4. Greitzer, F.L., Kangas, L.J., Noonan, C.F., Dalton, A.C., Hohimer, R.E.: Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In: 2012 45th Hawaii International Conference on System Science (HICSS), pp. 2392–2401 (2012)
5. Greitzer, F., Frincke, D.: Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In: Insider Threats in Cyber Security, vol. 49, pp. 85–113 (2010)
6. The Nikkoso Research Foundation for Safe Society: Research report for a measure of human factors threat to information security. The Nikkoso Research Foundation for Safe Society, Technical report (2010) (in Japanese)