Work 41 (2012) 2902-2907
DOI: 10.3233/WOR-2012-0542-2902
IOS Press

False alarms and incorrect rejections in an information security center: correlation with the frequency of incidents.

Thiers Bruno and Julia Abrahão *
Work and Organizational Social Psychology Postgraduate Department. University of Brasília (UnB). University of Brasilia. Central Institute of Sciences. Institute of Psychology. Room AT-013. Brasília, Brazil

Abstract. This study examines the actions taken by operators aimed at preventing and combating information security incidents at a banking organization. The work utilizes the theoretical framework of ergonomics and cognitive psychology. The method is workplace ergonomic analysis. Its focus is directed towards examining the cognitive dimension of the work environment with special attention to the occurrence of correlations between variability in incident frequency and the results of sign detection actions. It categorizes 45,142 operator decisions according to the theory of signal detection (Sternberg, 2000). It analyzes the correlation between incident proportions (indirectly associated with the cognitive efforts demanded from the operator) and operator decisions. The study demonstrated the existence of a positive correlation between incident proportions and false positive decisions (false alarms). However, this correlation could not be observed in relation to decisions of the false-negative type (incorrect rejection).

Keywords: Cognitive ergonomics, Information security, Signal detection, Alarms, Rejections

1. Introduction

The operational cost reduction and the increase in profits that made products and services available through internet banking and automated teller machines (ATM) accelerated the process of transferring retail operations from banks to virtual environments (Menezes & Bruno, 2007).

The internet banking and ATM channels together accounted for more than half of all banking transactions undertaken in the country (Brazilian Federation of Banks, 2010).

Classified by banks as information security incidents, attacks from hackers on these virtual environments evolved in frequency, strategies and operational methods. Currently, banks and financial institutions have expert teams working full time with supervision and prevention of these occurrences (Menezes & Bruno, 2007).

The overall aim of this study was to examine the operators in action at a supervision nucleus concerned with information security incidents in a Brazilian bank. The cognitive demands of the task were observed with special focus on the occurrence of correlations between the frequency of incidents and the results from the sign detection actions produced by the operators.

The signal detection theory (Sternberg, 2000) is usually associated with the study of vigilance and attention. According to this theory, four consequences are possible for attempts to detect an expected signal, which can be categorized as follows:

Table 1
Signal detection theory. Categories of decisions

	Respond Present	**Respond Absent**
Signal Present	True Positive	False Negative
Signal Absent	False Positive	True Negative

* Corresponding author. Emails: thiersdf@hotmail.com, julia.abrahao@gmail.com

The *false positive* (false alarm) and *false negative* represent subsets of the general errors (overall).

As the main focus of the research was to study possible correlations between the frequency of incidents and the results of detection actions, the specific objectives were:

a) Examine the correlation between the frequency of incidents and the number of false positive results (false alarms) in a certain period;

b) Examine the correlation between the frequency of incidents and the number of false negative results within the same period.

It was noticed that the activities of monitoring and detection performed by the operators in this complex socio-technical systems (Pavard, B. & Dugdale, J., 2006) demanded cognitive events related to memory, evocation of representations, problem resolution, decision-making and vigilance.

These events are used for the analysis of each incident. Thus, the increased frequency of incidents enhances the demand of such cognitive events or alternatively intensifies the cognitive demands for the operators.

According Amalberti (2007), recognition of the importance of cognitive demands on computerized tasks leads to realistically accept the risk, without belief in the utopia of inexistence of the failure.

The test about the existence of proportional correlations between the types of errors and the variability of incident frequency was made by using an independent variable, herein named *Incident Frequency*.

2. Method

This research is classified as a case study, in which the methodological procedures of the ergonomics analysis of work (EAW) are applied according the model proposed by Guérin *et al*. (2001). A case study (Leedy, 1997) allows analyzing complex phenomena involving people, processes, and events.

The method of choice for the Ergonomic Analysis of Work is justified by its flexibility, which allows iterating and the return to previous steps, leading to a progressive understanding of the analyzed situation (Abrahão et al., 2009). Apart from this, the various instruments to collect information in compliance with the methodology make its application suitable to the case studies.

Instruments like open interview, semi-structured interviews, overall observations, systematic observations, participatory and non-participatory observations, questionnaires, registers of speeches, and forms of data collection were used.

The research hypotheses were:

Hypothesis 1: There is a correlation between the frequency of incidents and the quantity of false positive decisions;

Hypothesis 2: There is a correlation between the frequency of incidents and the quantity of false negative decisions;

The results from decisions made by the operators were collected during a 60-day period. The correct decisions, false alarms, incorrect rejections and correct rejections were quantified. The variable behavior analyses were performed using an appropriate statistic model to assess the correlation between different variables (Beta regression).

The dependent variables were the following:

Table 2
Research variables.

Dependent variables	
False Positive	Proportion of false alarms
False Negative	Proportion of incorrect rejections
Overall	Proportion of total errors (false positive + false negative)
Independent variable	
Incident frequency	Daily frequency of incidents

An appropriate statistical model that identifies the proportions and correlations between the independent variable (*Incident frequency*) and the dependent variables (*false positive*, *false negative, overall*) was employed.

3. Results

The information security center population comprised 35 operators and 4 managers. Five operators were female. The activity was performed on a full-time basis (24 hours/day x 7 days/week). Educational indexes pointed to 82.05% of the population holding an undergraduate degree.

In average, the operators obtained results of the "True" type (*true positive* and *true negative*) in 77.2% of the decisions, though with a greater variability if compared to "False" results (*false positive* and *false negative*), as displayed in Table 3 and Figure 1. A maximum score of 183 *false negative* in one day was reported, which corresponds to 25.5% of the incidents. Figure 1 shows the daily evolution of such incidents. Up to the 42nd day, the evolution of incident proportion is more stable, with a slight variation around a general average for every

incident type. On the 43rd day, the proportion of successful trials leaps over 90%, but the proportion of correct rejections is significantly decreased as well, so the proportion of positive results remains practically steady.

Knowing he dependence level between *false negative* and *false positive* (alarms) and the total number of incidents is an issue of interest. Figure 1 shows the behavior presented by the proportion of *false negative* and alarms for each level of the number of incidents.

The proportion of *false negative* is apparently constant as the cognitive effort is intensified. The same does not occur to the proportion of alarms. It is possible to observe that the greater the cognitive effort, the greater the proportion of alarms (Figure 2).

In order to statistically confirm such evidences, three beta regression models for the following general formula were estimated:

$$f(y) = \mu + \beta x + \varepsilon \quad (1)$$

Where y is the dependent variable with Beta distribution (α, β), μ is the intercept, β is the parameter to be estimated, x is the independent variable (*Incident frequency*), and ε is the aleatoric error with average zero and constant variance.

These are the dependent variables of the models: proportion of total errors (*Overall = false negative + false positive*), proportion of *false negative* and proportion of *false positive* (alarms). This type of regression was chosen because the dependent variables (proportions) assume values in the gap (0.1). Therefore, the level of correlation among the three dependent variables and the frequency of incidents can be evaluated individually.

The results of the estimated models are presented in Table 4.

The significance level determined for the research was 0,05 in statistical applications (Gauvreau, K., & Pagano, M., 1994.).

The *Overall* and *false positive* variables presented significance within the gap of 0.004 and 0.001 so the correlation between these dependent variables and the independent variable can be taken into account (*Incident frequency*).

On the other hand, the *false negative* variable test presented a p-value of 0.601, which is above the level of significance established for the statistical test. Therefore, the existence Therefore, the existence of an relationship of the *false negative* variable with the independent variable (*Incident frequency*) cannot be considered..

The hypotheses tested by the statistical method were as follows:

Hypothesis 1: A correlation between *Incident frequency* and quantity of *false positive* occurred within a given period of time;

Hypothesis 2: A correlation between *Incident frequency* and quantity of *false negative* occurred within a given period of time;

When a total measure of errors represented by a variable known as *Overall* (*false negative* + *false positive*) (Table 4) is under study, it is possible to notice the existence of correlation between the frequency of incidents and the proportion of total errors. This correlation presents a positive nature. This means that the greater the number of incidents, the greater the proportion of general errors.

Through beta regression, the estimated models showed that the *Incident frequency* had a positive correlation with the proportion of *false positive*. However, the proportion of *false negative* remained unchanged as the number of incidents was increased.

The R^2 value presented by the Alarms variable confirms the independent force exerted by the independent variable over the correlation observed in relation to the Alarms variable.

Meanwhile, it is not appropriate to presuppose that it is possible to estimate models with a high predictive power owing to the limited number of variables used in the present study.

The test was limited to examining the possible correlations between the independent variable and the dependent variables that were taken into account.

The study demonstrated that a positive correlation is found between the variability of false Alarms and the frequency of incidents within the margin of error established as acceptable. By admitting a positive relationship between the frequency of incidents and the cognitive effort required from the operator, it is possible to establish and indirect correlation between the intensification in the emission of false alarms (*false positive*) and the intensification of cognitive demands. On the other hand, the correlation between the variability of incident frequency and the *false negative* cannot be observed. This points to the fact that the proportion of this error category would remain constant even through cognitive effort intensification.

Table 3

Descriptive statistic of the variables and proportions

Variable	**Minimum**	**Maximum**	**Mean**	**Standard Deviation**
True Positive	74	435	269.5	97.6
False Positive	5	347	158.3	99.4
False Negative	0	183	24.4	29.0
True Negative	3	593	300.2	161.3
True Positive (%)	19.8	91.6	38.7	12.8
False Positive (%)	0.7	35.1	19.1	8.6
False Negative (%)	0.0	25.5	3.7	4.4
True Negative (%)	1.3	75.6	38.5	14.8

Table 4

Results of beta regressions

Dependent variable	**Independent variable**	**Estimated coefficient (*Incident frequency*)**	**Standard error**	**z**	**p-value**	**Pseudo R^2**
Overall	*Incident frequency*	0.001	0.000	2.9	0.004	0.166
	Intercept	-1.819	0.207	-8.8	<0.001	
False Positive	*Incident frequency*	0.001	0.000	4.1	<0.001	0.245
	Intercept	-2.390	0.231	-10.3	<0.001	
False Negative	*Incident frequency*	0.000	0.000	-0.5	0.601	0.004
	Intercept	-3.135	0.241	-13.0	<0.001	

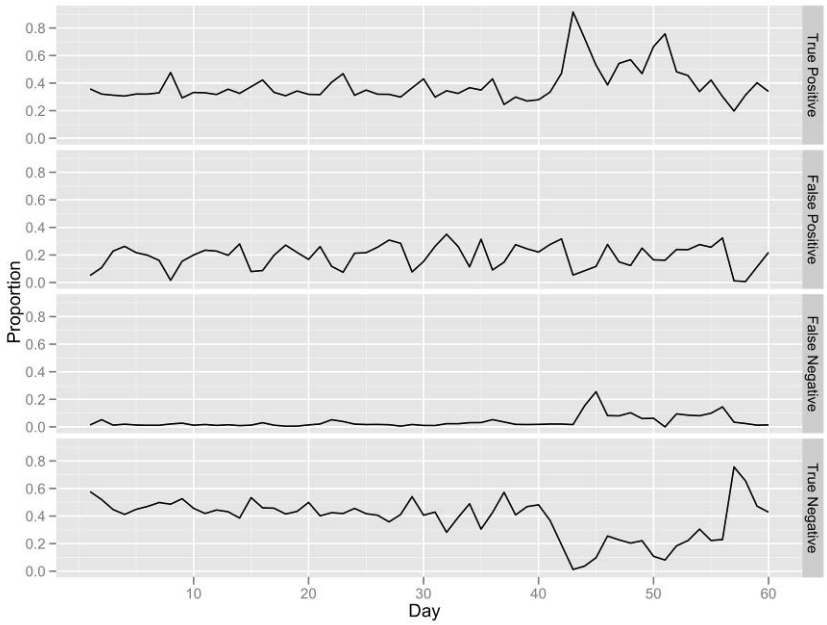

Figure 1. Proportion of incidents by type and day.

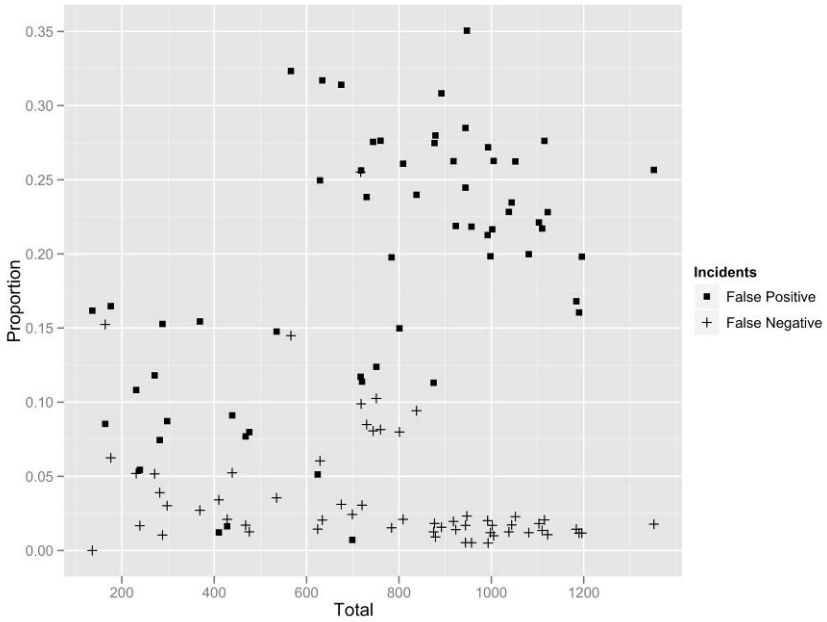

Figure 2. Proportion of false positive and false negative by number of incidents.

4. Conclusion

The study demonstrates that the activity performed by the operators is marked by concentrated attention (vigilance) and the intense production of representations towards action. Temporal pressure and fear from committing mistakes within the decision-making process contribute to aggravate the cognitive dimension of the activity.

The statistical Beta regression model, which analyzed 45,142 decision-making records concerned with testing research hypotheses revealed the existence of a positive correlation between the independent variable *Incident frequency* with the dependent variable *false positive*. Such relationship indirectly points to a positive correlation between the intensification of cognitive demands required for task accomplishment and the sending of false alarms.

However, the same correlation was not disclosed as *false negative* results were put into test.

Such phenomenon might as well be explained by admitting that other independent variables that might bring about the phenomenon were neither identified nor used within the scope of the present study.

Throughout the research, a few objects were acknowledged to deserve deeper investigation. Nevertheless, faced with the previously arranged objectives and considering the established deadline, such deeper investigation could not become real and ended up as proposals for future studies.

Future research could be directed to further understanding the phenomenon in particular, which involves the proportions of *incident frequency* and decisions of the *false negative* type, while other independent variables should be added.

The use of one more independent variable would be favored by the statistical modeling in use. In addition, it would increase the independent power of the methodology.

References

[1] Abrahão, J., Sznelwar, L., Silvino, A., Sarmet, M., Pinho, D. (2009). Introdução a Ergonomia: da prática à teoria. São Paulo. Edgard Blücher.

[2] Amalberti, R. (2007). Da gestão dos erros à gestão dos riscos. Em P. Falzon (Ed.). Ergonomia (pp. 235-247). São Paulo. Blücher.

[3] Brazilian Federation of Banks / FEBRABAN (2010). The banking sector in numbers. FEBRABAN. Disponível em: http://www.febraban.org.br/p5a_52gt34+5cv8_4466+ff145afbb52ffrtg33fe36455li5411pp+e/sitefebraban/Setor_Banc%E1rio_N%FAmeros_Junho_2010%20%282%29.pdf

[4] Gauvreau K, Pagano M. (1994). Why 5%? Nutrition,10(1), 93-94.

[5] Guérin, F., Laville, A., Daniellou, F. Duraffourg, J. & Kerguelen, A. (2001). Compreender o trabalho para Transformá-lo: A prática da Ergonomia. (tradução de L. Sznelwar et al.). São Paulo: Edgar Blüncher. (original publicado em 1991)

[6] Leedy, P. D. (1997). Practical research: planning and design. T. J. Newby e P A. Ertmer. 6 Ed. New Jesrsey: Prentice Hall.

[7] Menezes, W. J., Bruno, T. C. M. (2008). Análise Ergonômica de um Núcleo de Segurança Lógica. Trabalho apresentado no 15º Congresso Brasileiro de Ergonomia, 6º Fórum Brasileiro de Ergonomia e 3º Congresso Brasileiro de Iniciação em Ergonomia – ABERGO JOVEM. Porto Seguro (BA).

[8] Pavard, B. & Dugdale, J. (2006). The contribution of complexity theory to the study of sociotechinical cooperative systems. In A. Minai & Y. Bar-Yam (Eds.). Unifying Themes in Complex Systems, (pp.39-48). Massachusetts (USA): Springer Complexity/NECSI.

[9] Sternberg, R. J. (2000). Psicologia Cognitiva. Porto Alegre: Ed. ARTMED.