Do Organisational Security Measures Contribute to the Detection and Reporting of IT-System Abuses?

J.M. Hagen and P. Spilling

Gjøvik University College, Gjovik, Norway
University of Oslo, UNIK, Oslo, Norway
e-mail: janne.hagen @hig.no, paal@unik.no

Abstract

The paper presents a study of IT systems abuses, based on 390 responses from the Norwegian Computer Crime Survey 2006, and qualitative data from personal interviews of 94 employees in four enterprises required to obey the Norwegian Security Act. The aim of the study has been to shed light on a handful organizational security measures that contribute to the detection and reporting of security incidents. The results confirm significant positive correlations between organizational security measures and reporting of IT abuse incidents. But personal beliefs and judgements of the observed security breaches, however, influence the willingness to report colleagues to security management. Moreover, the results show that the reporting regime in Norwegian enterprises is too loose and the punishment too low to confirm any strong deterrent effect on employees, and most IT abuse incidents are regarded to be insignificant and not considered as criminal incidents.

Keywords

Computer crime, incident reporting, information security

1. Introduction

The current study focuses on abuse of IT systems performed by employees, and the use of organizational security measures to counteract such behaviours. Abuse of IT systems is a problem for all organizations; it includes among other things illegal downloads of software onto the IT systems, with increased exposure to malware infections like viruses, Trojan horses, and rootkits. IT abuse can also be unintentional and performed by accident. The study is based on data from the Norwegian Computer Crime Survey, 2006 (NCCS 2006). The findings are supplemented with qualitative analysis of responses from personal interviews with 94 employees in four Norwegian organizations with strong security regimes.

Our study was inspired by Wiant (2005); in order for a deterrent security measure to be effective, both the number and the severity of the computer abuse incidents should be reported. While Wiant viewed the security policy as a deterrent measure, our work is dedicated to detective and deterrent security measures, which are directed at IT users and naturally follows from the organizational security policy (Sterne, 1991). The study addresses the following two research questions:

1. Can organizational security measures directed at IT users, improve the detection probability and reporting of IT system abuses?
2. Is the applied punishment strong enough to have a deterrent effect?

This paper is structured as follows: first we review related work on the insider threat and leading and lagging indicators. In section 3 we present our two surveys and the research method. The results of our analysis are presented in section 4. In section 5 we discuss the findings. Section 6 concludes the paper.

2. Related studies on IT abuse and measurement indicators

Pearson and Weiner, 1985, give an overview of crime theories that provide different reasons for performing criminal activities. In this study, we have chosen to focus on the general deterrence theory (GDT), which asserts that the probability of illegitimate behaviour varies inversely with the perceived likelihood of being detected and the magnitude of punishment. According to this theory, few criminal activities are irrational. The GDT is well established in criminology and it has also been applied successfully to information systems (Straub and Nance, 1990; Straub, 1990; Straub, Carlson and Jones, 1992, Wiant, 2005).

The literature on computer crime and security breaches provides several reasons for misbehaving employees. The first reason is explained by both the human nature itself and by the lack of competence (Vivien, Thompson, Geok, 2002; Zhang, Oh, and Teo, 2006) or by the person's working conditions, such as the systems and security technologies they must use. The low level of usability of security solutions, such as passwords and PGP encryption, may prevent a correct use of the technology (see Florêncio and Herley, 2007; Whitten and Tygar, 2005). Perrow (1984) argues that huge system complexity and close interconnections make system failures inevitable. Kraemer and Carayon (2007) found in their study of five work-system elements, where sixteen network administrators and security specialists emphasized organizational factors as communication, security culture, and organizational structures as the most important reasons for human errors in computer security.

The second reason that employees have in dealing with information security, involves handling conflicting goals set by the management. Information technology users will overlook or ignore security concerns when such tasks interfere with or prohibit the completion of their work tasks: such omissions simply make it easier to do their job (Besnard and Arief, 2004).

The third reason, which an employee may play in regard to information security, is that of a disgruntled employee who wants attention, revenge, or to cover vandalism, or gain personal profit (Keeney et al., 2005). Halibozek and Kovacich (2005) argue that, in every reorganization process, there is at least one disgruntled employee, because in reorganizations, mergers, and downsizings, some employees are typically rewarded while others are downgraded or dismissed. This creates a bad working environment.

A forth reason is that of industrial espionage. On famous case in the United States was when Hitachi tried to get an IBM employee to sell the drawings for a next-generation computer (Boni and Kovacich, 2000).

Measuring IT abuse performed by insiders could be done by applying both leading and lagging indicators. Lagging indicators are measures of a system taken after the incident has occurred. They measure outcomes and occurrences (Grabowski et al, 2007; Beatham et al, 2004). In contrast, leading indicators aim to measure events that precede an undesirable event and have some value in predicting the arrival of the event. Leading and lagging indicators differ in granularity and focus. Leading indicators often have a focus on individual and perhaps departmental level, while lagging indicators have their focus on company or site level (Grabowski et al, 2007). Schultz (2007) present a framework that defines relevant types of insider-related attack behaviour that include deliberate markers, meaningful errors, preparatory behaviour, verbal behaviour and personality traits. The measurements are on individual levels, corresponding to the description of leading indicators (Grabowski et al, 2007). The NCCS 2006 provides data on an organizational level, thus enabling analysis of associations for identifying lagging indicators. This corresponds with most key performance measures, which are lagging indicators that do not provide the opportunity to change (Beatham, et al, 2004).

3. Methods and data

The data consists of two sets: (1) The Norwegian Computer Crime and Security Survey 2006 (NCCS 2006), and a total of 390 responses to a set of questions on computer abuse and punishment (Hagen, 2007, and 2008). The latter set of data resulted from personal interviews with 94 employees in four different organizations, on detection and reporting of computer breaches committed by colleagues (Hagen, 2008). We applied a stratified statistical sampling so that the respondents represented a cross-section of all employees and positions; the human resource manager picked employees from various departments of the organizations holding a variety of positions.

When interviewing the respondents, questions were asked about security violations they had heard about or witnessed. We also asked about their attitudes and practice of reporting security breaches, committed by colleagues, to the management as required by the security policy.

While Wiant (2005) studied the correlation between security policy and the reporting of incidents, our study has been focused on possible relationships between a few commonly applied security measures derived from the organizational security policy and directed towards the individuals in the organizations. Second, our study focuses on the practice for reporting of incidents, and finally on the chosen punishment.

Applying Straub's (1990) definition of deterrent measures, and extending Wiant's (2005) approach with a more detailed view of the implementation of the security policy, we identified 6 deterrent organizational measures in the Norwegian Computer

Crime Survey directed at influencing employees' behavior. These are: (1) application of user guidelines, (2) non-disclosure agreements that employees must sign, and (3) education of IT users to raise security awareness. We also include in the analysis the incident response plan (4) and practice/culture of reporting computer crime incidents to the management (5), and also the practice of checking logs frequently (6). We use Spearman Correlation Analysis to study correlations between deterrent organizational measures and the binary lagging indicator of having reported at least one IT abuse incident or not. Furthermore, we use qualitative data for the purpose of triangulation; i.e the data collected by either method can be used to validate the other (Hamersley, 1996).

4. Research results

4.1. Reporting of abuse incidents by enterprise size

The reported IT abuse incidents for the organizations are shown in Table 1. A chi-square test confirms significant differences at 5% level among the three enterprise size categories: small, medium and large. The overall majority of the 390 enterprises report to have no abuse incidents. Forty-three of the 390 respondents reported a total of 94 security violations. The table also shows that a larger portion of large enterprises report to have one or more IT abuse incidents compared to smaller enterprises. The results show that among the 43 enterprises that reported IT abuse, 12 perpetrators were external consultants and 31 were own employees.

Enterprise category	**Percentage of enterprises reporting different numbers of abuse incidents**							**N**
Reported number of incidents	*0*	1	2	3	4	5	10	
Small enterprises < 25 employees	96.9	2.1	1	0	0	0	0	195
Medium sized enterprises	90.3	3.4	2.8	2.3	0	0.6	0.6	176
Large enterprises >200 employees	83.2	9.2	4.2	0.8	0.8	0.8	0.8	119
Total number of reported incidents within each reporting category	0	21	24	15	4	10	20	94
Enterprise reporting incidents within each reporting category	347	21	12	5	1	2	2	390

Table 1: Reporting of computer abuse in Norwegian enterprises

The qualitative data show that one out of 94 employees had ever witnessed a serious computer crime incident performed by a colleague. However, what was judged to be minor security omissions or breaches were far more commonly reported: from 4 to 13 percent of the employees had reported a security breach last year to the security management. This is well in line with the findings of Table 1.

4.2. Use of deterrent security measures and reporting of incidents

Formalistic measures such as user guidelines and non-disclosure agreements are most frequently used, while educating the IT users are rarer. Few enterprises have an incident response plan, and also a practice or a culture of reporting incidents. Statistical analysis of the survey show that there are significant differences at 5%

level in the use of deterrent measures between small, medium sized enterprises and large enterprises, as shown in Table 2.

Security Measures	**Enterprises that have implemented measures**		
	Small enterprises	Medium sized enterprises	At least 500 employees
User guidelines	44%	75%	92%
Non-disclosure Agreement	32%	46%	60%
User education	33%	48%	51%
Incident Response Plan	8%	28%	54%
Reporting of incidents	15%	23%	49%
Frequently checking logs	55%	72%	91%

Table 2: Percentage of enterprises applied formalistic security measures

Hypo-thesis	**Security Measure**	**Spearman correlation**		**Partial correlation controlling for enterprise size**	
		Spearman's σ	**Significance level**	**Partial correlation coefficient**	**Significance level**
1	User guidelines	0.19	0.00	0.12	0.00
2	Non-disclosure Agreement	0.16	0.00	0.13	0.00
3	User education	0.1	0.83	-0.02	0.65
4	Incident Response Plan	0.16	0.00	0.09	0.04
5	Reporting of incidents	0.16	0.00	0.11	0.01
6	Frequently checking logs	0.14	0.00	0.09	0.05

Table 3: Correlations between security measures and abuse reporting (N=390)

Table 3 shows that there are positive correlations between deterrent organizational information security measures and reporting of IT abuses, even when we correct for enterprise size. These deterrent measures are user guidelines and non-disclosure agreements. Some of the measures come into force after an incident has occurred, i.e. log checking, incident response plan and the practice of reporting incidents to management. Moving over to the 94 qualitative responses, they indicate a gap between a good attitude to report incidents and what actually happened when an incident is observed. Reporting depends on how serious the consequences are, who the perpetrator is, and whether the action can be characterized as human error or intended action. New employees report security breaches more often than experienced employees: 26 percent versus 12 percent. It is somewhat surprising that user education does not turn out to correlate significantly with the detection of IT abuse, as we expect user education to increase general awareness.

Finding 1: User guidelines, Non-disclosure agreements, and Reporting of incidents are the most effective organizational information security measures to detect and report IT abuse.

4.3. Consequences and punishments

The strongest punishment measure is probably to be reported to the police or being dismissed. When the security has been violated by an internal employee, there are two more or less independent aspects to consider. One aspect is the time needed to bring the system back into a secure state. This includes analysis of the security violation, determine the information that has been compromised, determine who caused the problem, and possibly upgrade the security functionality and the security policy. The other aspect relates to the system and its stored information that has been manipulated or lost, as a result of the security violation. The system and its information must be brought back to its secure state. The results show that of the 21 enterprises that answered the question, 11 recovered and restored the system within 2-3 hours, and 20 within one day. We have no indication on how much of that time has been used to analyze the security incidents themselves, but we know that only one organization consulted experts.

Finding 2: Most of the organizations used less than one day to recover from the IT abuse incident, and only one consulted an expert; thus the consequences are reported to be manageable by own resources.

Among the 31 enterprises, 22 answered the questions of reporting the IT abuse as a criminal offence to the police: Only two enterprises reported a total of 3 IT abuse incidents as a criminal offence to the police. Thus the probability of being reported to the police is limited. The main explanation was that the crime was not judged to be serious enough to be reported to the Police. Five enterprises dismissed the perpetrator as a consequence, or brought the case to the court.

Finding 3: The probability for severe punishment for IT abuse is low.

5. Discussion

5.1. Why do employees misuse and abuse IT systems?

The crime theory explains criminal behaviour from several perspectives, such as sociological, psychological, economical and ecological (Pearson and Weiner, 1985). The computer crime literature reveals that there are several reasons for employees to not comply with security guidelines: ordinary human errors that occur as a result of human nature, lack of knowledge (Vivien et al., 2002; Zhang et al., 2006), system complexity and low security usability (Florêncio and Herley, 2007; Whitten and Tygar, 2005; Perrow 1984), the conflict between achieving business objectives and complying with security requirements (Besnard and Arief, 2004), or cost benefit evaluation of outcome driven by malicious motives such as revenge, greediness etc (Keeney et al., 2005). To the latter, according to the GDT, employees will not commit crime if the probability of being caught and the punishment outweighs the expected benefits. These two variables can be manipulated by management, and the current study shows how the majority of Norwegian enterprises do not regard the consequences of IT abuse committed by own employees as significant enough to

report the offence to the police or dismiss the perpetrator. The deterrent effect of such a regime is probably small, which in turn may lower the barriers for abusing IT systems, compared with other kind of crime, ex stealing money.

The qualitative data shows that far from all security breaches are reported. Most are dealt with personally or overlooked, because they are not serious enough. There are several reasons that employees do not want to report a colleague: lack of knowledge, the consequences are judged to be too small, and the intent was not regarded to be malicious, or the perpetrator was a manager and the employee fear the personal consequences or personal disagreement with the strict security regulations.

5.2. Can organizational security measures, directed at IT users, improve the probability of detecting and reporting IT system abuses?

According to (Mitropoulus et al, 2005; Randazzo et al, 2004, Keeney et al, 2005) the employees are important for the detection capability of an organisation. To be effective, deterrent measures should be well known by the IT users and appropriate punishment should follow any violation of the rules (Wiant, 2005). Studying our results, we find that several awareness-raising measures, such as user guidelines and non-disclosure agreements, correlate positively with reporting of IT abuse incidents. These measures are examples of practical implementations of security policies, and according to Höne and Eloff (2002; Kemp, 2005), the practical implementation is important for the effectiveness of the security policy. Also some measures that follow after an incident correlate positively with reporting of IT abuses. These include reporting to management, incident response plan and log checking. Such measures show that the organization has a reaction force when incidents appear. However, the qualitative responses indicate that far from all computer crime incidents are reported, even if they are in fact detected. Most employees prefer to speak directly to the colleague, if he or she breaks the security rules, unless it is judged to be very serious incidents. There is a clear personal evaluation of the consequences of the crime and the intent behind the incidents before any incident is reported to management. Also, frequent log checking may not normally reveal security violations. The normal user activities, like web surfing, emails, and downloading of information, may overshadow “normal” activities were infected material are imported. It will therefore be difficult to detect such activities on a general surveillance basis. The low correlation coefficient may explain this.

Our findings support the findings of Keller et al (2005); larger enterprises will normally devote more resource to protect their sensitive information, hence implement more sophisticated security measure and thereby increase their power to detect abuses than small businesses. There is, however, no significant change between large and smaller enterprises with respect to IT user education. Also, surprisingly, we find no significant correlation between user education and the detection of IT abuse. One possible explanation is that user education is of varying quality.

5.3. Is the applied punishment strong enough?

Norwegian enterprises do not use strong sanctions to punish employees that commit IT abuse, but the punishment corresponds with how the management evaluate the consequences. The deterrent effect is probably low because the probability of being punished is low and the punishment itself is weak. These findings are in line with that of Albrechtsen and Hagen, 2008. They compared the use of organizational security measures with the practice within the safety management discipline, and found that the last way of solving a security problem, sanctions, dismissal or relocation of employees, is used rarely. Holding the findings up with the qualitative responses given by the 94 respondents, it seems obvious that most employees do not fear any punishment of misbehaviour, and they seem to be aware that there is a lot of slack in the organization, and room for personal adjustments. What is judged to be a serious IT abuse, however, is reported to the police.

5.4. Limitations

The NCCS 2006-survey data are typical lagging indicators, collected at an organizational level. The qualitative study based on the 94 personal interviews, aims to get further insight into human psychology and leading indicators. The kind of serious computer abuse incidents, however, are very rare.

The non-response of the NCCS 2006 survey reached 63% (749 responses). Our data set were further reduced to 390 respondents who answered the questions of IT abuse, giving a response rate of 19.5%. It is still enough data to reveal significant differences between the groups of enterprises and to study correlations, and the findings are representative for the Norwegian companies.

Respondents may be reluctant to report computer crime incidents, out of fear for their own reputation. CSI/FBI and PWC document that companies do not report computer crime incidents, out of fear for their reputation. To mitigate this, the Norwegian Computer Crime and Security Survey provided anonymity. Besides, the correlation analysis is conducted on binary data rather than the number of reported incident. This is considered to strengthen the validity of the result.

6. Conclusion

In this study, we have chosen to focus on the general deterrence theory (GDT). Starting this study, we judged two relevant, but alternative approaches; one behaviouristic approach with focus on deterrent security measures, and one more in line with modern management ideas focusing on human resources. Because of the kind of data available in the NCCS 2006, the reported IT abuse incidents, we chose the behaviouristic approach and applied an analytical approach with similarities to (Wiant, 2005).

The aim of the current study has been to uncover which organizational security measures that contributes to the detection and reporting of security incidents and

what kind of penalties that are imposed. We found that there is a positive and significant correlation between some organizational security measures and reporting of IT abuse incidents, although the correlation coefficients have low absolute values. The qualitative responses confirm an underreporting of security breaches whenever a colleague is involved, even if the security policy and guidelines require reporting, no matter what. So far the reporting regime in Norwegian enterprises is too loose and the punishment too low to confirm any strong deterrent effect on employees, and most IT abuse incidents are regarded to be insignificant. Emphasis should rather be on building awareness and good attitudes towards correct usage of IT systems.

Our study indicates that the probability of detection can be improved, by implementing a wide range of organizational detective and deterrent security measures. This can improve the statistics on computer crime, which is fundamental for determining the effectiveness of security investments and to conduct risk analysis.

7. References

Albrechtsen, E., and Hagen, J (2009) "Information Security Measures Influencing User Performance," in Martorell et al., eds., *Proceedings of Safety, Reliability, and Risk Analysis: Theory, Methods, and Applications*, 2009, 2649-2656.

Beatham, S., C. Anumba, T. Thorpe, and Hedges, I (2004), "KPIs: A critical appraisal of their use in construction," *Benchmarking: An International Journal*, 11:1, 2004: 93-117.

Besnard, D. and Arief, B (2004), "Computer security impaired by legitimate users", *Computers and Security*, 23 (34), 2004: 253-264.

Boni, W., and Kovacich, G. L (2000), *Netspionage: The Global Threat to Information*, Boston: Butterworth-Heinemann, ISBN 0-7506-7257-9.

CSI/FBI *Computer Crime Survey*, 2005.

Florêncio, D., and Herley, C. (2007) "A Large-Scale Study of Web Password Habits," *Proceedings of the Sixteenth International World Wide Web Conference (WWW2007)*, Banff, Alberta, May 8-12, 2007, 657-656.

Grabowski, M., Ayyalasomayajula, P., Merrick, J., Harrald, J.R., and Roberts, K. (2007) "Leading indicators of safety in virtual organizations", *Safety Science*, 45 2007, 1013-1043.

Hagen, J.M. (2007), *Evaluating applied information security measures: An analysis of the data from the Norwegian Computer Crime Survey, 2006*, Norwegian Defense Research Establishment (FFI), FFI-rapport 02558, 2007, 1-66.

Hagen, J. (2008) "How do employees comply with security policy? A comparative case study of four organizations under the security act," in review, *Journal of Information System Security*, 2008.

Halibozek, E.P. and Kovacich, GL (2005), *Mergers and Acquisitions Security*, Elsevier Butterworth-Heinemann, Burlington, USA, 55-89, ISBN 0-7506-7805.

Hammersley, M (1996), "The relationship between qualitative and quantitative research: Paradigm loyalty versus methodological eclecticism". In: Richardson JTD (ed) *Handbook of qualitative research methods of for psychology and social sciences,* Leicester, UK, the Brittish Psycological Society, ISBN 1 85433 204X.

Höne K. and. Eloff, J.H.P (2002), Information security policy – what do international security standards say?, *Computers & Security*, 21 (5), 2002, 402–409.Keeney, M.; Kowalski, E, Capelli,

D., Moore, A., Shimeall, T. and Rogers, S., (2005), *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, May 2005, Carnegie Mellon, Software Engineering Institute.

Keller, S., Powell A., Horstman B., Predmore, C., and Crawford M (2005): "Information Security Threats and Practices in Small Businesses", *Information Systems Management*, Spring 2005, 7-19.

Kemp, M (2005), "Beyound trust: security policies and defence in depth", *Network Security*, August 2005, 14-16.

Mitropoulos, S., Patsos, D. and Douligeris, C (2006), "On Incident Handling and Response: A state-of-the-art approach", *Computers & Security*, 25, 2006, 351-370.

NCCS 2006, *Mørketallsundersøkelsen om datakriminalitet 2006* (The Norwegian Computer Crime Survey 2006), Næringslivets sikkerhetsråd (in Norwegian).

PWC, PriceWaterhouse Coopers, DTI information security breaches survey. Technical report, 2005.

Randazzo, M.R, Keeney, M.; Kowalski, E, Capelli, D. and Moore, A (2004), *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance sector*, August 2004, Carnegie Mellon, Software Engineering Institute.

Sterne, D.F. (1991), "On the Buzzword 'Security Policy'", Research in Security and Privacy, 1991. *Proceedings, 1991 IEEE Computer Society Symposium*, 219–230.

Straub, D. J. Jr,; (1990), "Effective is security, an empirical study", *Information Systems Research*, 1 (sep, 01) (3), 1990, 255.

Straub, D.W, Carlson, P.J. and Jones E.H. (1992), "Deterring highly motivating computer abusers: a field experiment in computer security." In. G.G. Gable and W.J. Caelli, editors, *IT-security, the need for international cooperation*, North Holland, Amsterdam (1992), pp 309-324.

Straub W.D, and Nance, W.D (1990), "Discovering and disciplining computer abuse in organizations: a field study," *MIS quarterly*, 14, (Mar 01, 1990), (1), p 45.

Schultz, E.E (2002), "A framework for understanding and predicting insider attacks, " *Computers and Security*, 21 (6), 2002, 526-531.

Vivien, K.G.L, Thompson, S.H.T. and Geok, L.L (2002) "Cyberloafing in an Asian context: How do I loaf here? Let me count the ways," *Communications of the ACM*, 45:1 (2002): 66-70.

Whitten, A., and Tygar, J.D. (2005) "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in L. Cranor and S. Garfinkel, O'Reilly, eds., *Security and Usability: Designing Secure Systems that People Can Use*, , 679-702, ISBN 0-596 00827-9.

Wiant, T.L (2005), "Information security policy's impact on reporting security incidents," *Computers & Security*, 24, (6), September 2005, 448-459.

Zhang, D., Oh, L-B. and Teo, H.H (2006), "An Experimental Study of the Factors Influencing Non-Work-Related Use of IT Resources at Work Place," *Proceedings of the 39th Hawaii International Conference on System Science*, 8, 2006: 206.1.