Security issues in distributed financial information systems: case of Greece

Dimitrios I. Maditinos [a], Željko Šević [b] and Nikolaos C. Kokkinos [c*]

[a] Kavala Institute of Technology (KIT), School of Business and Economics, Department of Business Administration, Ag. Loukas, 65404 Kavala, Greece
E-mail: dmadi@teikav.edu.gr

[b] Glasgow Caledonian University, Business School, Cowcaddens Road, Glasgow G4 0BA, UK
E-mail: Zeljko.Sevic@gcal.ac.uk

[c] Kavala Institute of Technology (KIT), Faculty of Engineering, Department of Petroleum & Natural Gas Technology, Ag. Loukas, 65404 Kavala, Greece
E-mail: nikokkinos@mwpc.gr

Abstract: The significance and the susceptibility of financial data make the security of financial information systems (FIS) a major and simultaneously, neuralgic concern for every enterprise; especially, when FIS control industrial plants. Last decade, the modern industrial FIS not only widely use distributed data processing (DDP) configuration, but also being more and more pushed by the demand of transferring information inside (from the shop to the top-floor in a typical factory scenario) and outside the factory (through public networks e.g. Internet). However, it is remarkable that the number of the threats and violations are increasing while technology is developing. Therefore, building efficient and safe FIS in industrial plants is not a trivial task, but it is a fundamental issue starting from the earlier phases of the design of a system and continuing with the adoption of diverse complex technologies. A survey in forty large industrial plants of Greece sheds light to the vulnerable points of security in distributed FIS. Thus, several in-depth interviews with the CIO (Chief Information Officers) and/or system administrators and also, observations on the spot took place in order to examine the security policy of the FIS in distributed computer networks. User authentication policy, audit trails events, CIOs'/system administrators' graduated studies are the mainly examined criteria in this study. The results revealed that the Greek companies need to realise and to take more seriously the fact that security is not something extra, but a normal part of performing business.

Keywords: Security, Financial information systems, Distributed networks.

* Corresponding author.

1 Introduction

Nowadays, advances in network technology and the globalisation of markets and business processes have created a revolution in business and information systems (Calderon, Chandra and Cheh, 2006). The well-known term "business" is converted to "e-business" ("e-" refer to various technology-enabled business activities) upgrading its main infrastructure. The main infrastructure for e-business consists of corporate computer networks that compose the backbone of distributed financial information systems (Prabhu and Raghavan, 1996). Nevertheless, Bertolotti *et al.* (2007) underlined that computer networks are exposed to serious security threats (attacks from hackers, malicious users or even cyber-terrorists, who use hi-tech abuse techniques and methods to commit computer fraud) that can even have catastrophic consequences from both the economy points of view and safety; especially, if computer networks control critical infrastructures, such as industrial plants. The basis of the above mentioned problem is the fact that the modern industrial information systems (which include networks between computers and intelligent devices from the shop to the top-floor of a typical factory scenario) are interconnected with public networks (e.g. Internet) which makes them vulnerable to common security threats (Romney and Steinbart, 2003; Bertolotti *et al.*, 2007). Subsequently, how secure, reliable, consistent and valid are the distributed financial information systems (FIS) in the Greek industrial plants? A survey in forty large industrial plants in Greece sheds light to the hidden points of view of security in distributed FIS. The observation of the technical network specifications as well as the analysis of the security policies of the examined firms are the main targets of the current study.

Though computer networks offer a lot of worthy of remark services and advantages, many expanded threats appear to the FIS and eventually, to the whole enterprise. It is remarkable that the number of the threats is increasing while the technology is developing (Allen *et al.*, 2000). Despite the fact that most employees don't even give a minute per hour of their workday for IT security (Luzwick, 2004), system security is a very important issue, which the chief information officers (CIO), system administrators, supervisors and managers ought to take it into serious consideration. In addition, system security also consists of many and various components. A user name and a password is only one of the known safety measures against expanded threats. Furthermore, there are a lot of other types of security, such as data encryption, routing verification procedures, intrusion detection etc. That is why a survey took place in order to examine specific factors that seriously affect the security of distributed FIS of several large enterprises. Throughout this survey, primary data were gathered from forty large industrial plants in Greece (several interviews and observations took place). The password policy, audit trails events, the use of Kerberos system and CIO's/system administrator's graduated studies were examined in this work.

2 Theoretical Background

2.1 Financial Information Systems (FIS)

The main obligation of FIS is to keep updated and under control not only the revenue, the expenditure, the production and the human resources/payroll cycle of a firm, but also the general ledger and the reporting system of a firm (Romney and Steinbart, 2003). Thus, financial information systems offer: operational assistance to a firm (keeping track of transactions), knowledgeable support (using computerised tools for quick and easy support in investments), managerial aid (controlling financial resources) and strategic development of the organisation (establishing long-term investments goals and providing long-range forecasts of the firm's financial performance). The above features of FIS are achieved and integrated with the widely use of distributed data processing (DDP) configuration, as well as the use of enterprise resource planning (ERP) system applications. ERP systems integrate all the operational aspects of a firm with the traditional accounting-financial functions. The corporate data are kept in databases and a database management system (DBMS) is responsible for the data exploitation and sharing. Romney and Steinbart (2003, p. 335) mentioned that "in response to the Y2K issue, many large organisations replaced their disparate stand-alone legacy systems with integrated information systems, such as enterprise resource planning (ERP) systems". Nowadays, it has been observed that there is a wide use of ERP systems by most of the contemporary enterprises (O' Mahony and Doran, 2008).

2.2 Secure password policies

The Securing Proprietary Information Committee of the American Society of Industrial Security observed that the value of a company's future lies not in its tangible assets, but in the "intellectual capital" of the business (Carter and Katz, 1997). In most businesses today, intellectual property is kept in computers by means of data, information and computerised processes. Crume (2004) cited that according to a survey by Barron McCann, 92 per cent of IT managers prefer to use passwords as protection from possible data thieves. This means that FIS are only as secure as the weakest password (Schneier, 2000, p. 139). Hacking or cracking can be slowed down significantly or even defeated through the use of strong passwords. According to Microsoft Security Guidance Kit (2004) and to SANS Institute Password Policy (2005), a strong password is a password that includes characters from at least three of the five groups in the character classes table (Table 1). In addition, the longer the password the more difficult it is to break. Crume (2004, p. 1) stated that "a 4-digitnumeric password could be cracked on a modest PC in 0.02 seconds -faster than you can blink your eyes". However, the longer the passwords are, the more difficult it is for the users to remember them (Warkentin, Davis and Bekkering, 2004; Schneier, 2000). Consequently, creating passwords with both complexity and length makes it the most difficult of all to break.

Table 1 Character classes table.

Group	Example
Lowercase letters	a, b, c, …
Uppercase letters	A, B, C, …
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /
Unicode characters	€, , *f*, and ?

Choosing a secure password is mainly a matter of individual responsibility and training, too (Cooper et al., 1995; Charoen, Raman and Olfman, 2005). Thus, a couple of secure password techniques have been developed in order to help end-users and system administrators to keep their passwords safe. One of the best secure password techniques is the use of smart cards (Hancock, 1999). These smart cards generate a new and unique password every minute. The information system uses the same algorithm and generates the same passwords, because it is time-synchronised with the smart cards. The specific password procedure requires a user to enter a value obtained from a smart card when asked for a password by the computer. Even though it is a better way of dealing with authorisation than with the traditional password approach, it is more expensive and maybe a little bit inconvenient to carry the smart card. Moreover, an alternative password technique which is based on the confidentiality of the systematically repeated change of passwords is the password age. The system administrators ought to adjust properly the maximum password age (in days). This adjustment determines how many days a password can be used before the user is required to change it.

2.3 Audit trails

Another security technique, which has been developed for FIS since the inception of computers, is audit trails (Allinson, 2001). Although in the beginning the audit trails were used in accounting for the checking of financial reliability of a business, nowadays they have become a process of recording a series of specific events occurred in an information system. Cooper *et al.* (1995) defined audit trails as any file that records the time users log in, from where they log in, what they try to do, and any other action a CIO might want to save for later analysis. In other words, audit trails can provide CIO with valuable information in tracking security violation and break-in attempts. Therefore, audit trails seriously contribute to a process verification of an information system, as well as to fraud prevention. Despite the important contribution of audit trails to information system security, an Australia wide survey in the Australian Commonwealth and State Governments revealed that most organisations approach audit trails with inconsistently and incomprehensively (Allinson, 2001).

2.4 Data encryption

Due to the extraordinary growth of the Internet and technology-enabled business activities, many organisations rely on encryption to protect sensitive information transmitted over the Internet and other networks. In the field of on-line applications and client/server computing, where the communications medium is TCP/IP, Kerberos

protocol is commonly used (the name comes from Greek Mythology). Kerberos is an authentication system that is part of project Athena at Massachusetts Institute of Technology - MIT (MiUen *et al.*, 1987) and it supports high level authentication in distributed information systems (Pfleeger, 2000). A user of a Kerberos enabled distributed FIS has the facility to log in once and uses a variety of services during a specific session, without the inconvenience of explicitly authenticating (Neuman and Ts'o, 1994). Kerberos has been adopted by many enterprises, universities and organisations, and implementations are available for all major operating systems (Butlera *et al.*, 2006).

3 Methodology

Taking into consideration the above-mentioned theoretical and empirical background, an integrative survey was designed and took place in forty Greek large industrial plants (Table 4, Appendix 1). The main purpose of the survey is firstly, to examine thoroughly the infrastructure of each industrial plant; and then, to focus on the specific security issues of the observed distributed FIS, individually.

The survey was conducted by in-depth interviews with the CIOs and/or system administrators and afterwards by several observations on the spot. Thus, a first contact type of e-mail with an attached automated-electronic form was sent to many CIOs, system administrators and IT consultants in Greece. The particular electronic form informed the receivers about the subject, the questions and the purpose of the interview. Then, each enterprise completed the form and sent it back to the author by e-mail. After the first data gathering by e-mail, several interviews (some of them by telephone communication, due to the big distances) with the CIO of the firms were arranged in order to illuminate every obscure corner of the study. In addition, in some cases the final verification of the corporate data was achieved by the author thorough observation of the current distributed network infrastructure of the examined FIS. Eventually, all the collected data (gathered by e-mails, interviews and observations) were structured, tabulated and encoded by two different statistical software applications in the Process Simulations and Statistical Analysis Labs, of the Department of Petroleum & Natural Gas Technology, of Kavala Institute of Technology.

The content of the above data gathering was orientated into two sections. In the first section, the technical specifications of the observed computer networks were identified in order to ensure the existence and the operational conditions of a distributed FIS. Thus, the geographical scope of the network, the network topology, the type of data communication cables, the nominal data network speed, the type of router, the number of corporate servers, the type of servers and clients depended on use, the CPU (Central Processing Unit(s)) and the NOS (Network Operating System) of the servers, the CPU and the OS (Operating System) of the clients were examined. In the second section of the collected data, a security approach of the above defined distributed FIS took place. Hence, the first factor that was investigated was the type of the password the users choose for accessing FIS resources. A sample of 30 per cent of the users within the examined companies who participated in this survey was studied (more than adequate for statistical analysis). Four types of password authentication were checked: simple passwords (insecure passwords, which have small lengths and homogeneous characters), complex passwords (passwords with both complexity and length), complex passwords with specific expiration date and

the use of smart cards (one of the best modern password techniques). The second examined security issue was the audit trail events of the FIS. Thus, five significant parameters were examined in the current survey: the audit trail generation, the audit trail retention, the audit trail storage, the existence of enhanced security mechanisms and the responsibility for audit trails (Allinson, 2001). Another examined security parameter was the use of Kerberos protocol in the FIS and the relation of CIO's/system administrator's graduated studies with the information technology field. With regard to the latter parameter, it is noticeable that in some of the examined firms the CIO and the system administrator were the same person; and in other cases, there was only a system administrator.

4 Results and discussion

The main criterion of the sample selection was the FIS of every large Greek industrial plant to be based upon a distributed computer network, which consists of a switched Ethernet type of local area network (LAN) with a gateway to the Internet (Figure 1). Thus, the first section of data gathering (concerning technical network specifications) took place in order to ensure that the sample followed the requirements of the study. According to the first section of data gathering, it was found that apart from the corporate LAN, ten of the forty firms also used a wide area network (WAN) or a metropolitan area network (MAN). Nevertheless, the above isolated cases used separated gateways, which were dedicated for WAN or MAN use. Therefore, the above phenomenon did not affect the current survey. Though, there was a significant amount of useful outcoming information from the technical network specifications of the examined industrial plants (first section of the survey), the main scope of this research paper is not computer science, but the security approach of distributed FIS (second section of the survey).

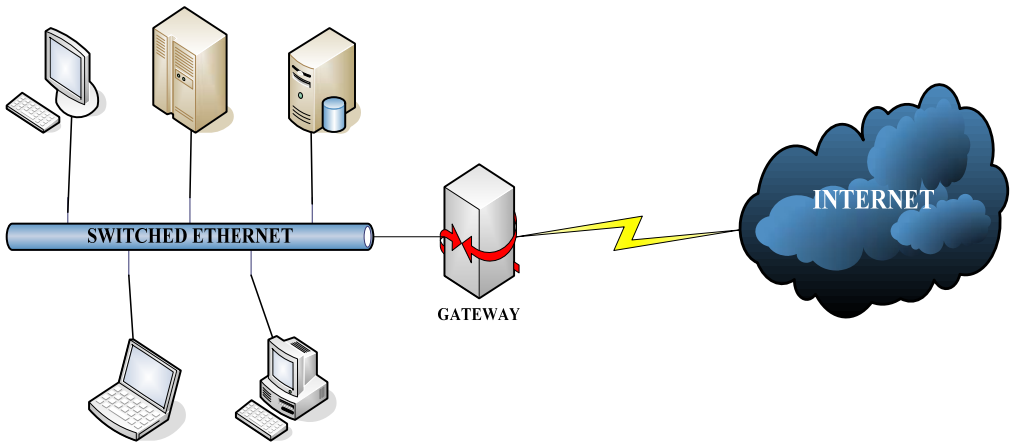

Figure 1 Network infrastructure of the examined distributed FIS.

The first examined security factor of the distributed FIS was the reliability of the password authentication, which was used by the 30 per cent of the users within the examined firms. The results revealed that the 32.5 per cent of the sample used simple passwords, 37.5 per cent used complex passwords and only the 30 per cent of the sample

used complex passwords with specific expiration dates (Figure 2). It is worth mentioning that 5 per cent of those who used simple password claimed that they knew how to make complex passwords, but they were afraid of forgetting them; and the remainder of them (27,5 per cent) claimed that they had never been trained to use "strong passwords". Another important finding was that the 30 per cent of those who used complex passwords did not use password age, because this option has been disabled by the system administrator; and the other 7.5 per cent disabled it by themselves for facility reasons. The lack of users' training and the lack of time of the IT support department occupied with expired passwords are in line with the theoretical background (Warkentin, Davis and Bekkering, 2004; Schneier, 2000; Charoen, Raman and Olfman, 2005). Furthermore, Table 5 (Appendix 2) shows that there is a significant statistical association between the IT graduated studies of CIO/system administrator and the level of security of users' passwords [$x^2(2)=10.95$, $p<.01$]. For instance, 92.3 per cent of the users, who used simple passwords, work in companies with non-IT graduates CIO/system administrators and the 66.7 per cent of the users, who used complex passwords with expiration date, worked in companies with IT graduates CIO/system administrators. The above observation reflects the fact that the users of the examined firms, whose CIO/system administrators were IT graduates, used more secure passwords than the users of the companies with non-IT graduates CIO/system administrators. Unfortunately, none of the examined enterprises used smart cards for password authentication; most of them believed that it was too excessive, expensive and also complicated technique.

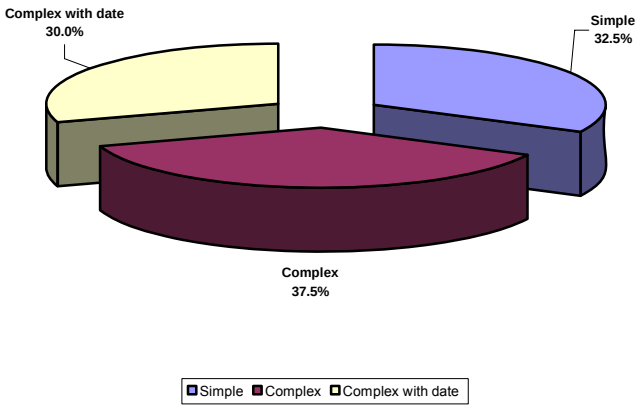

Figure 2 Type of password protection.

Audit trail was the next examined variable in the security of a distributed FIS. Five important parameters of audit trails were examined in this survey (Allinson, 2001). The generation of audit trails by the companies and the proper attention to them was the first examined parameter. In other words how many companies wittingly not only generate audit trails by the use of software tools, but also retrace them. According to Table 3 (Appendix 1) only 30 per cent of the companies generated audit trails and paid the proper attention to them. Many CIO/system administrators stated that they could not undertake

all the security-related duties they wanted due to the overwhelming daily FIS obligations. The next examined parameters (Table 3, Appendix 1) referred only to those companies that generate audit trails (i.e. 30 per cent of the initial sample). Thus, 66.7 per cent of the companies that generated audit trails retained them for up to 2 years and the rest of them for more that 2 years. Most of them (58.3 per cent) kept the audit trails on the same file server with the other corporate data, the 33.3 per cent used peripheral storage devices for audit trails retaining and only 8.3 per cent used a separated server for audit trails. Moreover, most of the firms (66.7 per cent) did not use security mechanisms (password authentication or data encryption) to protect the audit trails from unauthorised access; and only 33.3 per cent used password protection for accessing the folder of audit trails. The responsibility and the control of audit trails from a security perspective belonged equally to information system departments (41.7 per cent) and to system administrators (33.3 per cent); the responsibility for the audit trails of the remaining percentage belonged to the business owners, when none firm had established an audit department. Comparing the results of the companies that generated audit trails with the IT graduated studies of their CIO/system administrators (Table 6, Appendix 2) there is a significant relationship [$x^2(1)= 10.178$, $p<.01$]. This seems to represent the fact that based on the odds ratio ($odds\ ratio = \frac{odds_{non-IT\ graduate\ doesn't\ use\ AT}}{odds_{IT\ graduate\ uses\ AT}} = \frac{\frac{20}{8}}{\frac{2}{10}} = 12.5$) (Field, 2005) CIO/system administrators were 12.5 times more likely not to be IT graduates if they did not used audit trails than if they used audit trails.

Another important security factor examined of the distributed FIS was the adaptation of Kerberos authentication system by the Greek private industrial plants. However, in spite of the fact that Kerberos is a system that supports authentication in distributed systems, only 15 per cent of the examined sample used it (Table 2, Appendix 1). It seems that Kerberos is not a popular system in Greece and most of the firms did not use it, because they did not know it. Consequently, even though the name Kerberos comes from Greek Mythology, the Greek private industrial plants did not prefer to use the Kerberos authentication system in their FIS.

5 Conclusions

Taking everything into consideration, several useful and remarkable conclusions could be drawn from the current survey. The lack of users' training and the lack of time of IT support departments to spend on expired passwords are the main reasons that make users of a distributed FIS to use simple and insecure passwords. Moreover, the overwhelming daily FIS obligations force CIO/system administrators to be inadequate to their stern security-related duties as the audit trails generation and exploitation. In addition, the CIO/system administrators ought to stand not only upon their experiences, but also upon their educational provision. On the other hand, smart cards for password protection and Kerberos authentication system are not popular systems in Greece and most of the examined companies did not use them, because they did not even know them. Consequently, the Greek enterprises need to realise and take seriously the fact that security is not something extra, but a normal part of performing business. A better

allocation of the information system department's duties and also, the development of new IT departments that would be dedicated to specific duties, as audit trails, it would alleviate the CIO/system administrators' burden and make them more productive and efficient. Hence, it is really wise for every company to develop security policies and to use the proper security tools and techniques for achieving integrity, reliability, availability and accuracy of its financial information system.

References

Allen, J., Alberts, C., Behrens, S., Laswell, B. and Wilson, W. (2000) *Improving the security of networked systems*, Carnegie Mellon University's Software Engineering Institute, Pittsburg.

Allinson, C. (2001) 'Information Systems Audit Trails in Legal Proceedings as Evidence', *Computers & Security*, Vol. 20, No. 5, pp. 409-421.

Bertolotti, C. I., Durante, L., Maggi, P., Sisto, R. and Valenzano, A. (2007) 'Improving the security of industrial networks by means of formal verification', *Computer Standards & Interfaces*, Vol. 29, No. 3, pp. 387-397.

Butlera, F., Cervesatob, I., Jaggardc, D. A., Scedrovd, A. and Walstadd, C. (2006), 'Formal analysis of Kerberos 5', *Theoretical Computer Science*, Vol. 367, pp. 57-87.

Calderon, T.G., Chandra, A. and Cheh, J. J. (2006) 'Modeling an intelligent continuous authentication system to protect financial information resources', *International Journal of Accounting Information Systems*, Vol. 7, No. 2, pp. 91-109.

Carter, L.D. and Katz, J.A. (1997), *Computer crime: An emerging challenge for law enforcement*, Michigan State University, East Lansing.

Charoen, D., Raman, M. and Olfman, L. (2008) 'Improving end user behaviour in password utilization: An action research initiative', *Systemic Practice and Action Research*, Vol. 21, No. 1, pp. 55-72.

Cooper, J. F., Goggans, C., Halvey, J. K., Hughes, L., Morgan, L., Siyan, K., Stallings, W. and Stephenson, P. (1995) *Implementing Internet Security*, New Riders Publishing, Indianapolis.

Crume, J. (2004) *Inside Internet security - What hackers don't want you to know*, Addison-Wesley.

Field, A. (2005), *Discovering statistics using SPSS*, Second Edition, Sage Publications, London.

Hancock, B. (1999) 'Smart Card Security Users Group created to ensure highest standards of security', *Computers & Security*, Vol. 18, No. 8, pp. 653-654.

Luzwick, P. (2004) 'Security? Who's got time for security? I'm trying to get my job done', *Computer Fraud & Security*, Mayfield Press, Oxford, pp. 16-17.

Microsoft, Security Guidance Kit, CD-ROM edition, Spring 2004.

MiUen, S. P., Norman, C., Schiller, J. I. and Saltzer, J. H. (1987) *Kerberos authentication and authorization system, Project Athena Technical Plan, Section E.2.1*, MIT, Cambridge.

Neuman, C.and Ts'o, T. (1994) 'Kerberos: an authentication service for computer networks', *IEEE Communications*, Vol. 32, No. 9, pp. 33–38.

O' Mahony, A. and Doran, J. (2008) 'The Changing Role of Management Accountants; Evidence From the Implementation of ERP Systems in Large Organisations', *International Journal of Business and Management*, Vol. 3, No. 8, pp. 109-115.

SANS Institute Password Policy (2005), http://www.sans.org/resources/policies/Password_Policy.pdf.

Pfleeger, P. C. (1997) *Security in Computing*, Second Edition, Prentice Hall, Upper Saddle River.

Prabhu, M. M. and Raghavan, S. V. (1996) 'Security in computer networks and distributed systems', *Computer Communications*, Vol. 19, No. 5, pp. 379-388.

Romney, B. M. and Steinbart, J. P. (2003) *Accounting information systems*, Ninth Edition, Prentice Hall, Upper Saddle River.

Schneier, B. (2000) *Secrets and lies*, John Wiley and Sons, New York.

Warkentin, M., Davis, K. and Bekkering, E. (2004) 'Introducing the Check-off password system (COPS): an advancement in user authentication methods and information security', *Journal of Organisational and End User Computing*, Vol. 16, No. 3, p. 41.

Appendix 1. Frequency tables

Table 2 Frequency table of password, Kerberos use and IT Graduate security variables of the examined FIS.

Statistics				
		Password	Kerberos Use	IT Graduate
N	Valid	40	40	40
	Missing	0	0	0

Password				
		Frequency	Percent	Cumulative Percent
Valid	Simple	13	32.5	32.5
	Complex	15	37.5	70.0
	Complex with date	12	30.0	100.0
	Total	40	100.0	

Kerberos Use				
		Frequency	Percent	Cumulative Percent
Valid	No	34	85.0	85.0
	Yes	6	15.0	100.0
	Total	40	100.0	

IT Graduate				
		Frequency	Percent	Cumulative Percent
Valid	No	22	55.0	55.0
	Yes	18	45.0	100.0
	Total	40	100.0	

Table 3 Frequency table of the five parameters of audit trail security variable.

Statistics

		Audit trail generation	Audit trail retention	Audit trail storage	Enhanced security mechanisms	Responsibility for audit trails
N	Valid	40	12	12	12	12

Audit trail generation

		Frequency	Percent	Cumulative Percent
Valid	No	28	70.0	70.0
	Yes	12	30.0	100.0
	Total	40	100.0	

Audit trail retention

		Frequency	Percent	Cumulative Percent
Valid	<2Yrs	8	66.7	66.7
	>2Yrs	4	33.3	100.0
	Total	12	100.0	

Audit trail storage

		Frequency	Percent	Cumulative Percent
Valid	Peripheral Storage Device	4	33.3	33.3
	Separate files on same server as data	7	58.3	91.7
	Separate server	1	8.3	100.0
	Total	12	100.0	

Enhanced security mechanisms

		Frequency	Percent	Cumulative Percent
Valid	Not used	8	66.7	66.7
	Password protected folder	4	33.3	100.0
	Total	12	100.0	

Responsibility for audit trails

		Frequency	Percent	Cumulative Percent
Valid	System Admin	4	33.3	33.3
	Information system Dept.	5	41.7	75.0
	Business owner	3	25.0	100.0
	Total	12	100.0	

Table 4 Profile of the firms (number of employees, years of firms' experience in their field)

		Statistics		
		Employees		Experience
N	Valid	40		40
	Missing	0		0
		Employees		
		Frequency	Percent	Cumulative Percent
Valid	Less than 100	12	30.0	30.0
	100 to 199	20	50.0	80.0
	200 or more	8	20.0	100.0
	Total	40	100.0	
		Experience		
		Frequency	Percent	Cumulative Percent
Valid	Less than 5 years	4	10.0	10.0
	5 to 10 years	12	30.0	40.0
	More than 10 years	24	60.0	100.0
	Total	40	100.0	

Appendix 2. Cross-tabulations & chi-square analysis

Table 5 Cross-tabulation and chi-square analysis of variables: "IT graduated studies of CIO/system administrator" and "password".

			Password			
			Simple	Complex	Complex with date	Total
IT Graduate	No	Count	12	6	4	22
		% within IT Graduate	54.5%	27.3%	18.2%	100.0%
		% within Password	92.3%	40.0%	33.3%	55.0%
	Yes	Count	1	9	8	18
		% within IT Graduate	5.6%	50.0%	44.4%	100.0%
		% within Password	7.7%	60.0%	66.7%	45.0%
	Total	Count	13	15	12	40
		% within IT Graduate	32.5%	37.5%	30.0%	100.0%
		% within Password	100.0%	100.0%	100.0%	100.0%

(X^2=10.951, DF=2, p=0.004)

Table 6 Cross-tabulation and chi-square analysis of variables: "IT graduated studies of CIO/system administrator" and "audit trails".

			Audit trail generation		
			No	Yes	Total
IT Graduate	No	Count	20	2	22
		% within IT Graduate	90.9%	9.1%	100.0%
		% within Audit trail generation	71.4%	16.7%	55.0%
	Yes	Count	8	10	18
		% within IT Graduate	44.4%	55.6%	100.0%
		% within Audit trail generation	28.6%	83.3%	45.0%
	Total	Count	28	12	40
		% within IT Graduate	70.0%	30.0%	100.0%
		% within Audit trail generation	100.0%	100.0%	100.0%

(X^2=10.178, DF=1, p=0.001)