available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

The positive outcomes of information security awareness training in companies – A case study

Mete Eminağaoğlu [a,*], *Erdem Uçar* [b], *Şaban Eren* [c]

[a] *Yaşar University, Department of Computer Programming, Izmir, Turkey*
[b] *Trakya University, Department of Computer Engineering, Edirne, Turkey*
[c] *Yaşar University, Department of Statistics, Izmir, Turkey*

Keywords:
Information security management
Security awareness training
Password strength
Password usage
Password audit
Security awareness campaign

ABSTRACT

One of the key factors in successful information security management is the effective compliance of security policies and proper integration of "people", "process" and "technology". When it comes to the issue of "people", this effectiveness can be achieved through several mechanisms, one of which is the security awareness training of employees. However, the outcomes should also be measured to see how successful and effective this training has been for the employees.

In this study, an information security awareness project is implemented in a company both by training and by subsequent auditing of the effectiveness and success of this training (which focussed on password usage, password quality and compliance of employees with the password policies of the company). The project was conducted in a Turkish company with 2900 white-collar employees. Each employee took information security training including password usage. Also, there were several supporting awareness campaigns such as educational posters, animations and e-messages on the company Intranet, surveys and simple online quizzes. The project was carried out over a 12 month period and three password security strength audits were made during this period. The results were comparatively and statistically analysed. The results show us the effectiveness of the project and the impact of human awareness on the success of information security management programmes in companies. This study gives us some crucial results, facts and methods that can also be used as a guideline for further similar projects.

1. Introduction

In recent years, information security has received a lot of attention from various business areas, companies, enterprises, organisations and governments. Much of this can be attributed to an increase in security breaches leading to major losses suffered by the affected enterprises. Effective countermeasures, technologies, solutions usually exist for many of these breaches and related threats, but in most cases they are neither correctly nor effectively deployed. This is due to the fact that technology alone cannot deal with all information security risks, and the people in the organisations are actually the primary and the most critical line of defence (Tipton and Krause, 2007; IT Governance Institute, 2008). Much attention had been focused on technical aspects for dealing with information security management but less importance was given to people affected by these processes. However, this flawed reliance on technology is now changing; managers,

* *Corresponding author.*
E-mail addresses: mete.eminagaoglu@yasar.edu.tr (M. Eminağaoğlu), erdemu@trakya.edu.tr (E. Uçar), saban.eren@yasar.edu.tr (Ş. Eren).

1363-4127/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2010.05.002

security experts and all the other decision makers now primarily focus on people rather than technology. When it comes to the "human factor", there are various controls and most of these are related to training and education. Not only technical security training of IT staff, but also information security awareness training and other awareness campaigns have become a "must" for everyone. This fact has proven to be a mandatory criterion in international information security management system standards and related best-practices (Scholtz et al., 2006; ISO, 2005; Wood, 2002). People are the key factor to either success or failure of information security management in organisations. Every security breach or security problem is in fact associated more or less with humans, not only with technology. Any organization thinking of mitigating information security risks through purely technological countermeasures shall fail eventually (Mitnick and Simon, 2003). In any type of organization, each and every employee should be convinced and taught to contribute and comply with information security rules, implementations, and controls in order to achieve successful and effective information security management (Ashenden, 2008; Williams, 2008). In some of the studies and research, it has been shown that in order to gain such a contribution from employees, people must be subjected to proper awareness education and other awareness mechanisms and tools on a regular basis (Lacey, 2009; Gehringer, 2002). This has been the basic motive for carrying out a similar project in a Turkish company as explained in this paper.

2. Case study

This study was carried out as a project in one of the biggest transportation enterprises in Turkey. At the time of the project, the author of this study, Mr. Mete Eminağaoğlu had begun working as information security manager in this enterprise. There were around 3000 white-collar employees and 39 different companies within the enterprise. Although the core business was logistics and shipping, other companies were also present within the enterprise, e.g. tourism agencies, car resellers and insurance agencies. It should be noted that due to the privacy and security concerns of the company, formal names of the companies, people's names and the department names cannot be explicitly stated in this study.

2.1. *Initial situation: problems and needs*

In recent years, several major security incidents were experienced by the enterprise, mostly related with access control on IT systems. These incidents can be summarized as disclosure of some confidential data to some clients or other companies, erasing or changing some records by using another employee's access credentials and disclosure of all the employee salaries by accessing Human Resource files. These incidents were due to the misuse of users' access rights by giving away computer passwords, using very easy and simple passwords, leaving computer logon screens unlocked during lunch hours or after office hours. Throughout the company, computer passwords were the only technical security control. Most of the business processes and the IT systems were integrated on the MS Windows Active Directory domain system's authentication and authorization mechanism.

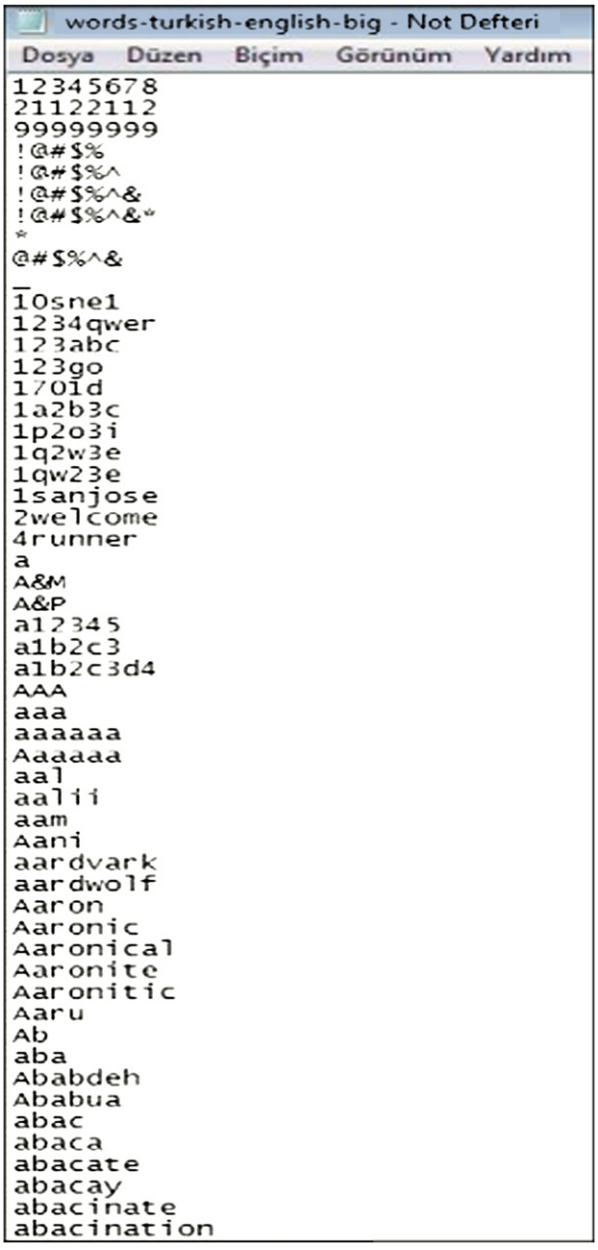

Fig. 1 – Excerpt from the dictionary file (including all English and Turkish words and specific patterns) used for dictionary attacks in the study.

However, senior management was aware of the actual reasons for these security breaches and sought proper and effective countermeasures to mitigate these breaches. It was also established that in most of these incidents, unintentional errors and ignorance were the main problems rather than intentional actions (intentional actions, e.g. disgruntled employees, sabotage, etc.). One of the primary concerns of senior management was to develop standards and compliance for proper use of passwords within the whole enterprise.

Fig. 2 – Excerpt from the dictionary file (including all English and Turkish words and specific patterns) used for dictionary attacks in the study.

At the time, there wasn't any ISMS (information security management system) within the enterprise and there were no formal written information security policies or procedures in the enterprise. No information risk analysis had been carried out in the enterprise. But, senior management was eager to establish ISMS programmes and they decided to start with password security.

2.2. *Information security awareness project*

Senior management's primary goal was to expand the proper use of passwords among the whole enterprise and to minimize the relevant risks. Establishment of an acceptable level of awareness among employees was the basic strategy in order to achieve this goal. This was decided by both the information security manager and other senior managers in the enterprise during the information security strategy meetings. All the necessary methods, projects, and the road-map for the related projects for an information security awareness campaign were also decided. As well as training, other sub-projects and methods were included within the awareness campaign.

2.2.1. *Strategy*

The strategy for an information security awareness campaign is summarized in this section. First, the current situation, previous relevant security incidents and their impacts, current risk levels (by a simple qualitative risk analysis) were analysed. Then, a technical audit of password weakness was conducted throughout the whole enterprise and the results and executive summary report were also analysed. Also, using these results, senior management derived basic objectives with some key performance indicators and key goal indicator values. (These values are given in Section 2.2.2.)

A detailed plan was prepared for the information security awareness campaign with all the necessary task times, deadlines and resources. Several countermeasures and projects for mitigating the relevant risks were put into the plan. The first projects were initiated according to the plan. All the required information security, access control and password policies and procedures were prepared and activated. Information security awareness training material and instructors were prepared and trainings began in several offices in parallel. In parallel with training, the other awareness tools and materials were also activated or distributed among employees. 6 months into the project, a second technical password security audit was conducted. Also, at the end of the first year, a third similar technical audit was conducted; at the same time a non-technical audit was carried out on some randomly chosen employees. All the results from these audits, together with feedback from the users, was collected and analysed by the senior management. All the managers had a chance to review the results, compare the results with their initial objectives and key goal indicators and decide whether it was necessary to look for further improvements.

It must be noticed that the whole strategy/phases within this project was very similar to the "PDCA – Plan, Do, Check, Act" model for information security management given in ISO27001:2005 (ISO, 2005).

2.2.2. *Project scope and objectives*

The information security awareness project's scope was defined and implemented as follows:

a. All white-collar employees in the enterprise participated in the training and in all the other awareness campaign activities.
b. Training sessions were carried out at 9 locations in 5 different cities.
c. All the technical password security audits were performed within all the MS Windows Active Directory user accounts in the enterprise.

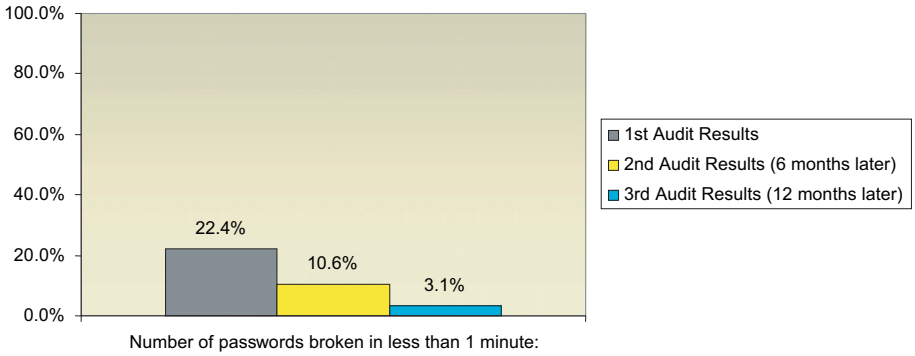

Fig. 3 – Comparative results from three audits: percentages of cracked passwords in less than 1 min.

The senior managers stated the project's objectives as follows:

a. The duration of the training project was exactly 1 year. After obtaining and reviewing the results for efficiency and effectiveness of the training, further training and/or additional awareness activities would be planned and implemented.
b. Within one year, all relevant information security policies and procedures should be approved and should be formally actioned.
c. As well as training sessions, all the other awareness campaigns within the plan should be activated.
d. By the end of the first year, at least a 30% decrease in very weak passwords must be observed (senior management concluded that passwords broken in less than 15 min are regarded as very weak).
e. By the end of the first year, at least 75% of employees within the enterprise should have been trained.
f. Among the randomly surveyed and audited employees, at least 50% of them should be using their passwords safely and properly and should be in compliance with the information security policies and procedures.

2.2.3. *Methods and tools used in the project*

Throughout this study and the related project, there were several sub-projects or activities coordinated and carried out in parallel. For some of these sub-projects or activities, some specific methods and tools were chosen and used. In this section we summarize these methods and tools.

For the information security awareness training, a team of experienced instructors from the training department and information security consultants within the enterprise were used. All of the training material was also prepared by this team. Each training course lasted 120 min (two sessions, each lasting 55 min and a 10 min break between the sessions). Each training group had between 16 and 40 employees. These employees were arranged in three different groups with alternative training modules. All the IT staff were organised in a special group and some technical aspects were covered in the course. All the department and company managers formed another group and their training was given by the information security manager in a single 60 min session. The remaining group attended the standard training module. In all of the training, not only password usage but also other concepts of information security that were essential for the enterprise were covered. The 120 min module included 30 min workshop.

Other information security awareness campaigns were also carried out as an enhancement to the training component. Posters containing slogans and graphics were prepared and hung on office walls. Some short web-based messages and flash animations were put onto the main internal web site and these were updated weekly or monthly. An information security portal on the corporate Intranet was also activated where corporate policies and procedures, simplified instructions (how to do, frequently asked questions) for secure usage of corporate IT systems, popular news, presentations, caricatures and videos (the latter ones acquired from free Internet resources),

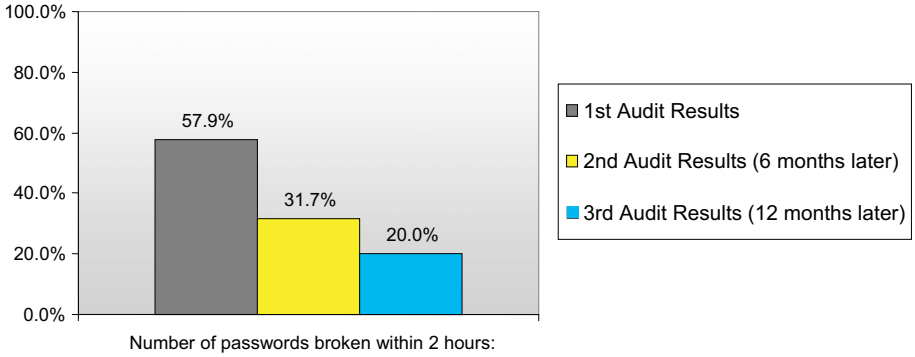

Fig. 4 – Comparative results from three audits: percentages of cracked passwords within 2 h.

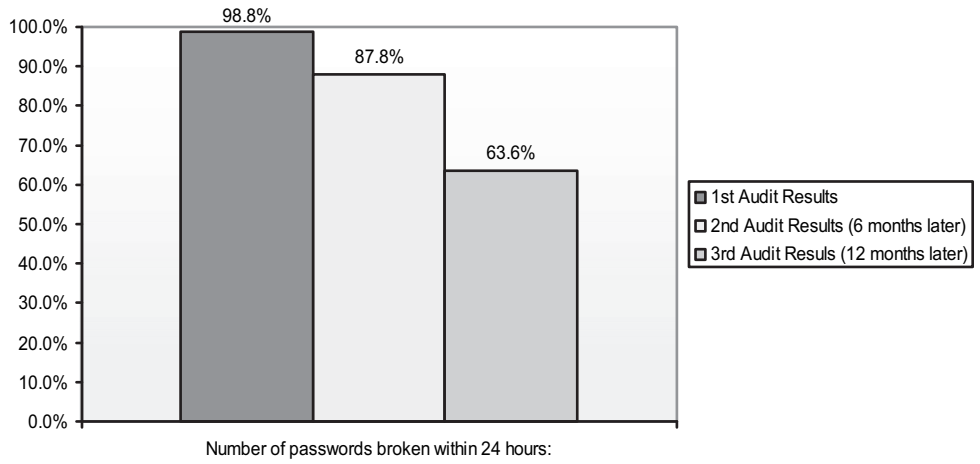

Fig. 5 – Comparative results from three audits: percentages of cracked passwords within 24 h.

interesting puzzles and quizzes were accessible to all the employees.

Another part of the project was password security audits. The first technical audit was conducted just before the project initialization. The other two technical audits were conducted after 6 months and again after 12 months of the project in parallel with training activities. In all of the technical audits the "L0phtcrack LC5" tool was used since it was one of the well known password weakness analysis tools for Microsoft Active Directory domain accounts (L0phtcrack LC5 Tutorial; Auditing User Accounts). This tool was installed on three different servers each with a configuration of Intel Pentium IV processors, 1 Gigabyte of RAM, 160 Gigabyte hard disks. Since, there are different password cracking (attacking) methods supplied within L0phtcrack, on each of the servers, a different attack mode (Dictionary attack, Mixed mode, Brute force only, L0phtcrack LC5 Tutorial; Auditing User Accounts; Pfleeger and Pfleeger, 2006) was chosen and the attacks were activated simultaneously. Dictionary attack is a type of cryptanalytic attack in which all the words in an extensive list (from a pre-arranged list of values, such as a dictionary) are sequentially tried as a possible password value. A brute force attack is another cryptanalytic technique where all possible combinations of the password (key) space are searched systematically (Pfleeger and Pfleeger, 2006). Another option in L0phtcrack combines a dictionary and brute force attack – so called mixed mode (L0phtcrack LC5 Tutorial). It should be noted that for the dictionary attack method in this study, L0phtcrack's built-in dictionary file was not used. Instead, an extended dictionary file was prepared and used. This dictionary file consisted of all the English and Turkish vocabulary words, some special department names from the enterprise and some specific patterns such as *12345678* or *1234qwer*. This dictionary file was composed of 257.551 distinct words and its total size was 2.927.101 bytes. Some screen shots of this file is shown in Figs. 1 and 2.

For all of the technical audits in this study, the longest dictionary attack lasted around 8 min. However, for the mixed mode and brute force only attacks, a 24-h time limit was used in the audits. This tactical decision was made because of two reasons. The first reason was that after 24 h, very few additional passwords (less than 10) would be cracked in the following days if the attack was continued. This wouldn't impact the audit results statistically, but on the other hand, this would prolong the audit process significantly. The second reason was that if any password was resilient to these attacks for more than one day then this was an acceptable and feasible threshold value for the senior management.

Table 1 – Summary of audit results for users' Microsoft Active Directory passwords.

1st Password audit results: (just before the project was initiated) Number of user accounts audited: 2846		% Broken (cracked) passwords
Number of passwords broken in less than 1 min	637	22.4%
Number of passwords broken within 15 min	1014	35.6%
Number of passwords broken within 2 h	1647	57.9%
Number of passwords broken within 24 h	2812	98.8%
2nd Password audit results: (6 months after the project began) Number of user accounts audited: 2911		
Number of passwords broken in less than 1 min	308	10.6%
Number of passwords broken within 15 min	715	24.6%
Number of passwords broken within 2 h	924	31.7%
Number of passwords broken within 24 h	2556	87.8%
3rd Password audit results: (12 months after the project began) Number of user accounts audited: 2924		
Number of passwords broken in less than 1 min	92	3.1%
Number of passwords broken within 15 min	203	6.9%
Number of passwords broken within 2 h	585	20.0%
Number of passwords broken within 24 h	1859	63.6%

Table 2 – Results from the first password audit: characteristics and percentages of the users' password choices.

Results from 1st audit: typical passwords		Percentages
12345678	341	12.0%
87654321	168	5.9%
Same as user account ID	76	2.7%
Special words (company name, Dept. name)	72	2.5%
Other words from dictionary	488	17.1%
Mixed patterns	1667	58.6%
Total no. of passwords cracked	*2812*	*98.8%*
PASSWORDS NOT CRACKED	34	1.2%
TOTAL AUDIT	2846	100.0%

During the project, as well as the technical security audits, some non-technical audits were conducted. At the end of the tenth month of the project, 190 employees were randomly chosen from two main offices and were asked to participate in short question–answer surveys and meetings. Some of these questions tried to establish the effectiveness of the awareness training; others focussed on more general aspects, e.g. what was the most interesting section in the company Intranet's security portal. Also, the same employees were observed during work hours (these observations focussed mainly on password usage). The results from the technical and non-technical audits were analysed and combined with feedback from the project participants. The resulting report, which included some statistical analysis, was presented to the senior management. Some of these results are given in Section 2.2.4.

2.2.4. *Results*

The main results are summarized below (these were also included in the executive summary report):

- 85% of all the white-collar employees in the enterprise attended the awareness training.
- 100% of the IT personnel attended the awareness training.
- 85% of the company and department managers attended the training.
- All the information security policies and procedures within the project scope were activated and applied.
- Six of the eight awareness activities were carried out.

Table 3 – Results from the second password audit: characteristics and percentages of the users' password choices.

Results from 2nd audit: typical passwords		Percentages
12345678	121	4.2%
87654321	73	2.5%
Same as user account ID	35	1.2%
Special words (company name, Dept. name)	54	1.9%
Other words from dictionary	459	15.8%
Mixed patterns	1814	62.3%
Total no. of passwords cracked	*2556*	*87.8%*
PASSWORDS NOT CRACKED	355	12.2%
TOTAL AUDIT	2911	100.0%

Table 4 – Results from the third password audit: characteristics and percentages of the users' password choices.

Results from 3rd audit: typical passwords		Percentages
12345678	29	1.0%
87654321	12	0.4%
Same as user account ID	4	0.1%
Special words (company name, dept name)	36	1.2%
Other words from dictionary	171	5.8%
Mixed patterns	1607	55.0%
Total no. of passwords cracked	*1859*	*63.6%*
PASSWORDS NOT CRACKED	1065	36.4%
TOTAL AUDIT	2924	100.0%

- Among 190 employees that were randomly chosen and audited, 114 of them complied with both the password policies and the other security policies/procedures.

Regarding the technical audits, L0phtcrack provided detailed statistics on users' passwords security levels and strengths. Summaries of these results are given in the tables below and in Figs. 3–5. The results of the three technical password audits show clearly that senior management's objectives were fully satisfied and even exceeded the estimated key goal indicator values. For instance, use of very weak password (broken within 15 min) decreased by at least 30% when compared with the initial objective. Table 1 shows that such passwords use was 35.6% before the project was started and after one year, this ratio dropped to 6.9%, which was far in excess of senior management's expectations and objectives.

The time ranges and the related results in Table 1 and in Figs. 3 and 4 are given as cumulative values. In other words, "cracked passwords within 2 h" includes all the passwords that were cracked either by brute force, by dictionary attack or mixed mode methods in at most 2 h (and therefore includes all passwords that were cracked in "less than 1 min" and "within 15 min").

In Table 1 and Figs. 3–5; the percentage values are derived from the number of cracked passwords divided by the total number of audited passwords.

In Table 1, the total number of passwords audited in the first, second and third audits are given as 2846, 2911, and 2924 respectively. These different values arise from employee turnover experienced during the duration of the project (Tables 2–4).

3. Conclusions

The results showed that the awareness training and other related campaigns did have positive and effective outcomes such as:

(a) Weak password usage was decreased significantly and continuously among most of the users.
(b) Employees began to develop a continual improvement of awareness and they had a inclined tendency to choose and use their passwords more safely.

(c) In addition to password usage, users began to participate in information security controls and mechanisms that were included in the awareness campaign.
(d) Most employees started to have (albeit reluctant) tendency to comply with the company's information security policies. This was also a crucial plus for the senior management.

We conclude that education and awareness is one of the most effective and powerful mechanisms for mitigating information security risks. In addition to training courses, there should also be various ongoing awareness campaigns complemented with supporting materials. This is due to the fact that most people might forget the concepts that they were exposed to during training. It is not effective and realistic to give the same training to people over and over again. Instead, users should be enabled with much more efficient and effective (in terms of time, money and impact) awareness materials such as posters, brochures, animated movies, animated electronic messages, online quizzes with prizes. All these materials must be designed by the relevant experts so as to make them user-friendly and attractive to employees. Visual materials (short, interesting, enjoyable movies, animations, caricatures, etc.) and short sentences are preferred rather than long, detailed, formal written materials (i.e., reports, articles, etc.). It must not be forgotten that information security should be easy, quick and simple to-understand, rather than being a burden ("another extra boring task"). User motivation, usability of both training materials and technical security control mechanisms are also a critical success factors for information security awareness programmes and information security management (Sasse et al., 2001).

Furthermore, within any information security programme or project, we must always audit, check and measure what we do or implement. This allows the efficiency and effectiveness of the security controls and solutions to be measured and analysed objectively. This approach will also help us to show which areas have improved, or point to potential changes in our information security management implementations and strategies. This fact, which is frequently mentioned in most of the international standards and related frameworks (IT Governance Institute, 2008; IT Governance Institute, 2007) has also been experienced in this study.

In each and every company and organization, regardless of its size, location, culture or type of business, "people" are always the key factor for the success of information security management.

Further case studies and similar research can be conducted in other companies where not only password usage but also some other security controls might be taken into consideration such as physical access, Internet access, mobile systems, document security, e-mail usage and so on.

REFERENCES

Ashenden D. Information security management: a human challenge? Elsevier Information Security Technical Report 13; 2008. p. 195–201.
Auditing User Accounts. Available from: www.windowsecurity.com/articles/Auditing-user-accounts.html.
Gehringer EF. Choosing passwords: security and human factors. In: ISTAS'02 international symposium on technology and society; 2002. p. 369–73.
International Organization for Standardization. ISO/IEC 27001: 2005. ISO; 2005.
IT Governance Institute. Information security governance: guidance for information security managers. ITGI Publishing; 2008.
IT Governance Institute. COBIT 4.1. ITGI Publishing; 2007.
Lacey D. Managing the human factor in information security: how to win over staff and influence business managers. John Wiley & Sons, Inc.; 2009.
L0phtcrack LC5 Tutorial. Available from: www.pdaapps.org/pc-softwares/13882-lopht-crack-v5.html.
Mitnick KD, Simon WL. The art of deception. John Wiley & Sons, Inc.; 2003.
Pfleeger CP, Pfleeger SH. Security in computing. Prentice Hall; 2006.
Sasse MA, Brostoff S, Weirich D. Transforming the 'weakest link' a human/computer interaction approach to usable and effective security. BT Technology Journal July 2001;19(No. 3): 122–31.
Scholtz T, Byrnes FC, Heiser J. Best practices and common problems for information security programs. Gartner; 2006.
Tipton HF, Krause M. Information security management handbook. Auerbach Publications; 2007.
Williams P. In a 'trusting' environment, everyone is responsible for information security. Elsevier Information Security Technical Report 13; 2008. p. 207–15.
Wood CC. Information security policies made easy. PentaSafe Security Technologies; 2002.

Mr. Mete Eminağaoğlu got his BS degree in the Department of Computer Engineering, Ege University, Turkey in 1996. He got his MS degree in 1999 in the Department of Computer Engineering, Izmir Institute of Technology, Turkey. Mete worked in the private sector for fourteen years as a Manager, Auditor and Consultant. He has CISSP and CISA certifications. He currently works as a Lecturer at Yaşar University, Turkey and he continues his PhD education at the Department of Computer Engineering, Trakya University, Turkey. His main research areas are information security risk modeling, adaptive algorithms, ISMS strategies and cryptography.

Dr. Mr. Erdem Uçar graduated from Department of Physics, Trakya University, Edirne, Turkey in 1992. He worked as a Research Assistant between the years 1991 and 1996 at the Department of Computer Engineering, University of Thrace, Greece where he also got his MS and PhD degrees in Computer Engineering. Mr. Uçar currently works as an Assistant Professor in the Department of Computer Engineering, Trakya University, Edirne, Turkey. He is also the Manager of Trakya University Computer Center. His main research areas are machine learning, information security management, medical Informatics and mobile applications.

Prof. Dr. Mr. Şaban Eren is the Dean of Faculty of Science and Letters of Yaşar University, Izmir, Turkey. He worked in the Computer Engineering Department of Ege University, Izmir, Turkey for many years and he was also the Chairman of the same department for nine years. His current research interests include IT security, statistics and software reliability. He has authored some national and international publications in the field of programming, office automation and statistics.