BEHAVIORAL APPROACH TO CORPORATE COMPUTER SECURITY

Dr. Haidar Fraihat
Mr. Ahmed Al-Ojairi
Accounting and Management Information Systems Department
King Fahd University of Petroleum & Minerals
Dhahran, Saudi Arabia

Abstract:
The purpose of this study is to find the causal impact of the prominent perception and awareness factors on employees' and managers' behavior concerning computer and information system security matters. For this purpose, a 3-modular questionnaire was developed. Factors related to the subject were divided into three main categories. (1) Awareness factors, (2) Perception factors, and (3) Behavioral factors.
The study results indicated that the awareness factors have a causal effect on the positive behavior of employees and managers toward computer security in organizations. It was found that perception factors have even stronger causal effect on the behavior of employees and managers towards observing computer security aspects.

"مدخل سلوكي إلى أمن حوسبة الشركات"

د. حيدر فريحات
أحمد العجيري

ملخص:
يهدف هذا البحث إلى دراسة تأثير كل من الإدراك والوعي بأهمية أمن أنظمة المعلومات في الشركات على سلوك الموظفين و المدراء المتعلقة بأمن أنظمة المعلومات. وعليه فقد تم تصميم استبانة ثلاثية النماذج اشتملت على العوامل الرئيسية المتعلقة بالموضوع حيث قسمت إلى ثلاثة مجاميع: (1) عوامل الوعي (٢) عوامل الإدراك (٣) عوامل السلوك. وجدت الدراسة أن عوامل الوعي لديها علاقة سببية على السلوك الإيجابي للموظفين و المدراء تجاه أمن حواسيب المنشأة. كما وجدت أن عوامل الإدراك لها علاقة سببية أقوى مع العوامل السلوكية المتعلقة بأمن حواسيب المنشأة. وعليه أوصت الدراسة بضرورة أن تراعى العوامل الادراكية وعوامل الوعي بمواضيع أمن أنظمة معلومات الشركات عند إعداد الاستراتيجيات والخطط والأنظمة والتعليمات.

Introduction:

Computers are increasingly becoming an indispensable tool in the day-to-day business operations as they became the core of many decision-making systems for public and private organizations alike. Computers have become such a valuable tools for today's business; however, the information age has also brought some potential problems for workers, organizations, and society. No information system operates in a vacuum. Furthermore, computer security, by all standards, is one of the biggest threats that are capturing the essence of many companies. One of the problems with computer security is that computer criminals are found at different levels: data processing operators, entry clerks, accounting personnel, programmers, supervisors and managers. Although no one really knows how pervasive cyber crime is, many agree that it is growing rapidly. Most all attacks go undetected, as many as 60 percent, according to security experts[1]. Big concerns are financial loss, loss of public trust and image and the fear of encouraging hackers by the lust of being challenged. Some crimes use computers as tools (e.g., to manipulate records, counterfeit money and documents, commit fraud via telecommunications links, and make unauthorized electronic transfers of money). Other crimes target computer systems, including illegal access to computer systems by criminal hackers, alteration or destruction of data and programs by viruses (system, application, and document), or even theft of computer resources. Today, computer criminals are becoming bolder and more creative than ever. With the increased use of the Internet and other network platforms, computer crime is becoming global. Security experts estimate that there are as large as 1,900 Web sites that offer the digital tools- for free- that let people snoop, crash computers, hijack control of a machine, or retrieve a copy of every keystroke[2].

It is often said that the only constant in life is change. Some changes are working in security's favor while others work against it. The use of computer security has developed over time in response to different needs and is capturing the essence of many companies. It is observed by many that most companies are concerned with the technical aspects of computer security. From a technical viewpoint, computer security is to "protect the physical items, objects, or areas of an organization from unauthorized access and misuse"[3]. While it is true that one can not have a completely secured systems without physical security at each of the access points, machines, network routers, network cable, etc., there is yet another important factor of security; the human element. From a managerial viewpoint, computer security may be viewed as the protection of information, systems, and hardware that use, store, and transmit that information. But, to protect information and systems from dangers, such behavior of individuals (insiders and outsiders) as they interact with systems as policy, awareness, training, and education are necessary.

Research Objectives:

The behavioral aspects of computer security are fast becoming one of the most important computer security issues of our information age. Although prior studies have identified

1 Stair and Reynolds, P. 557

2 Stair and Reynolds, P558

3 Whitman and Mattord, P9

factors that may lead to the importance of behavioral approaches in computer security, relatively little research specified an exhaustive list of parameters and tools that play a major role in assessing and measuring computer security. Here are the specific objectives of this research:

1) Emphasize the contrast between of the behavioral and managerial issues of computer security on apposed to technical issues.
2) Suggest managerial actions that can be taken to enhance the behavioral side of computer security in the work place.
3) Explorer the parameters that play the important role in assessing and measuring computer security issues.
4) Explore the means of predicting employees' behavior and corporate culture leading to or causing computer security breaches.
5) Examine the importance of computer security awareness among employees and how this varies across different segments of corporate employees.
6) Examine the level of computer security behavior among employees and how this can vary across different segments of corporate employees.
7) Examine the perception level of computer security perception among employees and how this varies across segments of corporate employees.

The importance of studying this subject is paramount. Many IT and non-IT managers usually emphasize the technical side of computer security and therefore give their full attention to procuring state-of-the-art technologies and establishing bullet-proof procedures for the purpose of enhancing the level of computer security in their organizations. While doing so, they tend to overlook and sometimes undermine a very important source of computer security breach, the human one. It is the intention of this paper to highlight the importance of the human aspects of computer security to management. The objective is to make CEO's and CIO's pay a well-deserved attention to the individual and group dynamics governing the work relations and work ethics within their organization and among their employees. If the right approach is to be adopted by concerned management aiming at encouraging positive employee behavior toward protecting the organizational information security and discourage negative attitudes, then, and only then, CIO efforts to mitigate computer and information security breaches will be successful.

Literature Review

It appears that most surveyed research dealing with computer security issues is focuses on the technical aspects. While early research focused on the technical part of computer security, more recent research has started to emphasize the human part of the issue. Some researchers proposed that treating security as an IT issue is a mistake that many businesses make. Moreover, they emphasize on the importance of the human side of computer security by stating that security problems are more often managerial than technical[4]. Paroby and Barrett outlined that password systems have proved to be difficult to manage and to be easily penetrated.[5] Catlett precisely viewed the laws to be more

[4] Robert W Scott, P17
[5] Paroby and Barrett, P40

effective than filters by saying: "Filtering is no more a solution to the spam problem than it is to water pollution. The right thing to do is to restrain the producers of pollution, rather than routinely burden someone downstream with the task of cleaning up an unfairly imposed mess. The cleanup task is necessarily an imperfect and expensive business"[6]. However, not all researchers agree with the idea of behavioral approaches in dealing with the computer security. Some argued that social controls are no longer effective deterrents, especially among employees occupying managerial positions in organizations[7].

The consequences of computer fraud are significant with estimates in 1994 as high as $9 billion a year in the U.S alone. However, no one knows the exact figure since most crimes go unreported. The majority of computer crime activities go unreported because companies fear bad publicity and future attacks by hackers who perceive a weakness in the company's security system. The FBI estimates that in 1998 only one percent of all computer crime is detected – other estimates range from 25%[8]. There are many types of computer fraud. One Study that examined cases of computer fraud found that 44% of computer fraud involves theft of money, 18% involves illegal trespasses, theft of services and other miscellaneous act, 16% involves damage to software, 12% involves alterations to data, and 10% involves theft of information[9].

Many researchers proposed that employees might be the greatest control strength, but they are also the greatest weakness[10]. Wright outlines that most computer crimes are committed by insiders[11]. Casabona and Yu precisely defined the percentage of computer crimes committed by insiders. They claim that between 85-90% of all computer security problems involve an unethical individual inside the corporation[12]. So, building a secure business does not stop with technological measures only. Preventing computer crime requires an understanding of human behavior. Scott views threats from employees as far more serious than intrusions by hackers. "It's the 15-- year-old hacker that makes big headlines," he observes. "But it's more often your 32-year-old disgruntled junior IT person who causes problems"[13]. Moreover, according to the Federal Bureau of Investigation, an astounding 85% of all computer security problems involve someone inside the corporation or organization[14]. Beyond that, some applied research from the consultants' domain has suggested that, if theft is defined broadly, 80 per cent of employees will steal under some circumstances[15]. The FBI's Computer Crime Unit reports that most acts of vandalism to data are inside jobs, performed by disgruntled employees with an agenda of their own-usually revenge[16]. So, it is clearly noted that

---

[6] Catlett and Graham, P57
[7] Wright, P56
[8] Casabona and Yu, P22
[9] Casabona and Yu, P23
[10] Wright, P57
[11] Wright, P56
[12] Casabona and Yu, P22
[13] Scott, P18
[14] Simpson, P43
[15] Wright, P56
[16] Simpson, P14

disasters stemming from unauthorized uses of either the system or specific types of data are internal threats and not limited to external ones. However, the insiders are not the only source of computer fraud. Casabona and Yu propose that outsiders as well as insiders within an organization are responsible for computer fraud[17]. It is also estimated that universities get from 10 to 30 hacking incidents each week[18].

The threats stemming from computer crimes have created new challenges for managers. Many business mangers are not prepared by attitudes or training to detect and prevent fraud, as noted by Casabona and Yu[19]. Thus, from their perspective, management of a business entity has a primary responsibility for developing internal control systems and ethics policies that will discourage fraud and reduce its occurrence[20]. Moreover, Casabona and Yu argued that the overall responsibility for a secured system usually falls to the systems analyst and often end-users[21]. In the same way, Simpson outlines the responsibilities of the IS department and managers toward computer security. From his point of view, IS department's responsibility is the physical safeguards and system management. On the other hand, managers must remain aware of user authentication and access control[22]. Still, getting management attention remains the major issue in making a business secure. This is because some researches stated that top managers have little concern for security issues, or tend to leave them to computer specialists[23]. Not only that but large numbers of corporations are not adequately prepared to deal with computer crime[24].

On the other hand, there are many behavioral reasons behind computer fraud in businesses. One of the most important ones is the lack of awareness in all organizational levels about the importance of computer security. Scott argues that most organizations are not aware of the risks they face. "They think by default that they are secure" [25]. In the same way, Wright found that younger people are less easily deterred from thievery[26]. One of the major reasons behind security problems is the lack of security policies. Moreover, Hannaford emphasized this point by stating that the lack of security policies has made it easier for computer criminals to carry out crimes[27]. Another reason behind poor security behavior within organizations comes from an ethical lack of understanding of the implications of one's actions[28]. In the same way, Casabona and Yu argue that people with low ethical standards are the heart of every computer fraud[29]. Employees of companies with comprehensive ethics programs know the law better than other company employees

[17] Casabona and Yu, P22
[18] Germain, P608
[19] Casabona and Yu, P24
[20] Casabona and Yu, P24
[21] Casabona and Yu, P24
[22] Simpson, P14
[23] Wright, P58
[24] Phillip C Wright, P58
[25] Scott, P 17
[26] Wright, P56
[27] Hannaford, P10
[28] Winn Schwartau, P 47
[29] Casabona and Yu, P24

and are more likely to report violations[30]. Some researchers refer security problems to the style of managing computer systems. For example, security problems at universities are more acute than governments' institutes because their computers systems are managed so loosely[31].

Some researchers proposed solutions for computer fraud problem from a behavioral point of view. In a survey conducted by the American Bar Association, respondents ranked specific requirements to prevent and detect computer crimes. The most important requirement proposed was to implement a more comprehensive and effective self-protection by private business. The second requirement was to push more education of users concerning vulnerabilities of computer usage. The next outlined requirement was to implement more severe penalties for fraud perpetrators. The last suggested requirement expanding education of the public about computer crime[32].

The main conclusion drawn from this survey of literature is that corporate management should carefully consider some important issues, other than buying more sophisticated applications and solutions. First of all it should be clearly stated that computer security is an issue of increasing concern. In the same way, security concerns are prevalent in all sectors of business, public and private. In addition, all organizations regardless of their size are currently facing security issues. Moreover, Security risks have increased in recent years and businesses are suffering financial loss because of security problems. The last main issue is that many organizations are just beginning to recognize the importance of adequate security. Security officers need help with establishing credibility for their security recommendations[33]. The following section is devoted to discussing the research methodology.

Research Methodology:

Since this research paper is concerned with the behavioral factors, it is felt that surveying existing IT practitioners in organizations at both management and non-management levels is an appropriate approach to achieve the research objectives. For this purpose, a 3-modular questionnaire was developed. Factors related to the subject were divided into three main categories. (1) Awareness factors, (2) Perception factors, and (3) Behavioral factors (see Appendix A). This classification was designed to better address the research questions. It is also in line with classifications of pervious research[34]. The initial research model is presented in Figure 1 below.

[30] Weiss, P18
[31] Germain, P610
[32] Paroby and Barrett, P 36
[33] Paroby and Barrett, P 44
[34] (Casabona and Yu, P22), (Scott, P18), (Simpson, P14), (Wright, P58), (Schwartau, P47),(Paroby and Barrett, P 36).

Top

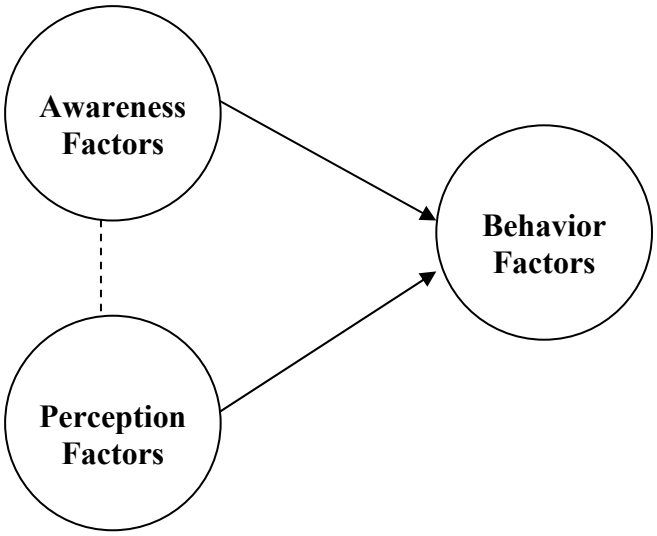

Figure1 Research Model

The purpose of this model is to indicate perception and awareness as factors affecting employees' and managers' behavior concerning computer and information security matters. This scheme will allow the researchers to compare the levels of importance of either of the awareness and the perception factors. If perception factors predominate, then CIO's would need to develop plans to mitigate any perception impairments. Likewise can be said about the awareness factors. All of the behavioral, perception, and awareness factors will also be tested against selected classifying factors such as employee demographical, educational and professional profiles. These as well as some factors related to the corporate environment in Saudi Arabian business culture will be tested as well. A series of descriptive statistics tools will be utilized in addition to some inferential statistical techniques such as Correlations and Regression (Single and multiple). The research model will then be tested based on the results of the statistical results.

Data Collection and Analysis:

As stated earlier, a questionnaire was developed and distributed to a sample of (60) respondents who are basically working full-time jobs mostly in managerial or technical nature at prominent large to medium-size organizations in Saudi Arabia. Some of these organizations are multinational ones. Summary of the major factors of the questionnaire are presented in Appendix (A). Most respondents were also part-time MBA students at the College of Industrial Management at KFUPM. This pool of participants guarantees diversified responses coupled with both personal integrity and professionalism. Out of the returned questionnaires, (3) were excluded because information was not complete enough. So, the sample size used in the analysis was (57). The Statistical Package for Social Sciences (SPSS) was used to conduct the needed statistics.

Top

Discussion:

Sample characteristics:

About 58% of the surveyed sample were in the second age group (26- 35 years), and 80% were Saudi nationals. The vast majority of the sample participant (more than 90% are holding at least a bachelor degree) so we can outwardly conclude that respondents belong to the literate strata of the corporate culture. About 62% of the participants belong to a medium salary bracket (between SR6, 000 and SR15, 000), however, only 21% received salaries more than SR15, 000. This indicates that salary should not be considered as factor in discouraging creativity and high productivity of managers regarding their work matters including computer security. Additionally, the analysis of the sample indicates that 17.5% of respondents are majoring in Management Information Systems, while 12.3% are majoring in Mechanical Engineering. Likewise, 12.3% are majoring in Construction Engineering & Management, and 12.3% are majoring in Civil Engineering. This means that about 55% of the participants are majoring in computer related majors. With regard to the previous experiences it was found that most participants (77%) have 6 years or less of experience in the organization. While 61% of respondents have less 3 years of experience in their current job and the remaining are having experience in their current job 4 years and above.

Table 1: Sample characteristics

	VARIABLES	PERCENTAGE (%)
Age	Below 25 yrs	١٤
	26 - 35 yrs	57.9
	36 - 45 yrs	22.8
	46 - 50 yrs	1.8
	Over 50 years	3.5
Nationality	Saudi	80.7
	Expatriate	19.3
Income	Less than SR 3,000	10.5
	SR 3,000- SR 5,999	7
	SR 6,000- SR 9,999	26.3
	SR 10,000 - SR 14,999	35.1
	SR 15,000 - SR 20,000	14
	Over SR 20,000	7
Major	Accounting	٧
	Finance	7
	Mechanical Engineering	12.3
	Construction Engineering & Management	12.3
	MIS	17.5
	Management	8.8
	Civil Engineering	12.3
	Computer Science	3.5
	Computer Engineering	7
	Others	12.4

	VARIABLES	PERCENTAGE %)
Managerial Level	Top	7
	Middle	36.8
	Operational	56.1
Experience in the Organization	1 – 3 yrs	43.9
	4 – 6 yrs	33.3
	7 - 10 yrs	5.3
	11 - 15 yrs	8.8
	16 - 20 yrs	5.3
	Over 20 yrs	3.5
Experience in the Department	1 – 3 yrs	61.4
	4 – 6 yrs	28.1
	7 - 10 yrs	3.5
	11 - 15 yrs	5.3
	16 - 20 yrs	0
	Over 20 yrs	1.8

Finally, it was found that more than half of respondents (56%) are currently holding an IT job at the operational management level, while about one-third of them in middle management positions, leaving only 7% in top management positions. Table1 summarizes the sample characteristics. From this table it can be easily concluded that the sample is fairly distributed among the various demographic educational and occupational factors.

Top

Awareness:
In all of the following analysis the score value (1) indicates strongly disagree, the value (3) indicates neutral response and (5) indicates strongly agree. With regards to the first awareness factor, two-third of respondents (67%) are found to be more or less aware of the general concept of computer security and (61%) understand the computer security policy in their organization and in the awareness factor regarding the "personal involvement in the design of computer security plans" results show that only (37%) of respondents were involved in the design of the computer security plans. However, (54%) were involved in the review and approval of the computer security policy. Additionally, about one-half of respondents (57%) believe that employees in the IT department use computer security measures before the rest the organization employees. With regards to management support it was found that (88%) of respondents believe that management support computer security policy. Table (2) summarizes the results of the awareness and other factors.

Perception:
Perception factors are designed here to gauge some of the believes, common understanding, and attitudes of respondents to selected computer security factors. For example, (65%) believe that the computer security issues are not exaggerated, indicating that computer security is a genuine issue. Accordingly, it was not surprising that (98%) of respondents believe that computer security measures benefit every one. And therefore, (90%) believe that money spent on enforcement of computer security is not wasted. With this notion (86%) of respondents believe that implementing a good computer security policy would improve the competitive advantage of the organization. With regards to the perception of protection measures to computer security threats, (72%) believe that enough is done in their organizations to protect their computers against threats. Accordingly, (84%) are confident that information systems in their respective organizations are well protected. However, (88%) of respondents believe that the government should make laws and regulations regarding computer security issues to support the policies and procedures adopted by corporations.

Table 2: Mean score of the awareness factors (A), the Perception factors (P) and the behavioral factors (B):

	Awareness	Mean	Std. Deviation		Perception	Mean	Std. Deviation
Awareness factors	**A1**	2.23*	1.21	Perception factors	**P1**	2.86	1.156
	A2	2.95	1.125		**P2**	4.32	.631
	A3	3.93	.977		**P3**	2.70	1.180
	A4	3.05	1.141		**P4**	2.19	.990
	A5	2.84	.902		**P5**	3.61	.959
	A6	2.67	1.024		**P6**	3.91	.950
	A7	3.33	1.006		**P7**	3.46	1.001
	A8	3.26	1.027		**P8**	3.88	.927
	A9	3.47	1.087		**P9**	3.32	.805
	A10	3.68	.890		**P10**	2.96	1.017
Behavior factors	**B1**	2.6	.97		**P11**	3.16	.996
	B2	3.3	.91		**P12**	3.35	1.009
	B3	3.9	.90		**P13**	3.07	1.033
	B4	3.6	.87		**P14**	2.75	.912
	B5	3.7	.89	* all values are statistically significant at alpha=5%			
	B6	3.6	.97				
	B7	3.1	.94				

Behavior:

The Behavioral factors depict that actual conduct with regards to observing computer security in one's organization. They have been carefully selected to indicate the actual organization practice of computer security measures (as opposed to perceptions or awareness). In this regard respondents provided their assessment of the current level of computer security behaviors in their organizations. It was found that (57%) of respondents agree (or strongly agree) that their organizations have a comprehensive ethics policy, and (60%) believe that their organizational culture is security conscious. More clearly, (94%) of respondents believe that ethics and good management practices will reduce not only the computer crimes but also the intensions to commit them. Finally, it was interesting to notice that most respondents (88%) believe that the computer security responsibilities are still been handled by middle or top management and not pushed down to the lowest managerial levels. This is a double-edged sword in the view of the researchers. From the one hand having IT being taken care off more at the top of the organizational hierarchy means more support to IT security policy and practice. On the other hand, Lower level management will be in the dark in terms of calling the shots for IT security policy formulation and implementation. So we might run into the risk of having a security policy that is not aligned properly with daily operational needs. This subject, although important, but it falls beyond the scope of this research.

Impact on the practice of computer security:
As stated in the research model presented in Figure1 and research methodology we will now assess the coherence and interaction among the awareness factors and among the perception factors. It was found (via testing the correlation among the variables) that there were 16 out of 81 statistically significant positive correlations between the awareness factors. These correlations were found to be significant at alpha = 5%. Furthermore, 37 positive correlations were counted at alpha = 10%. With regards to the perception factors 24 positive correlations were found among the 14 perception factors at alpha = 5% and 57 out of 98 positive correlations were significant at alpha = 10%. Total number of correlations for the perception factors was 98. The rest of the correlations among the awareness factors and perception factors are positive, however, at higher significance levels (alpha more than 10%). Very, few correlations were negative but without significance. With regards to the correlation between the awareness factors and perception factors, it was found that 20 out of 70 positive correlations were significant at alpha = 5%, and 39 positive correlations were significant at alpha = 10%. The remaining relationships were positive but significant at higher significance levels. Few negative correlations were found, however, without statistical significance.

It can be concluded from the above analysis that the two set of factors (awareness and perception) are in harmony with themselves and among each other. It can be added that the mean score of the awareness factors together was 3.141 out of 5 (Leaning to the agreement side). The same thing can be said to the mean score of the perception factors with score 3.253 out of 5. Both results were significant at alpha = 5%. This implies that most people are aware of the importance of the behavioral security issues and most of them understand the various peculiarities of the issues. Now that this is established we will move to assessing the relationship between the awareness and perception factors from the one side, and the behavioral factors on the other side.

To asses the causal relationship between the awareness factors and the behavioral factors the researchers used a linear step-wise regression model. Before implementing this statistical approach, the mean values of all of the behavioral factors were averaged out in one proxy variable (mean of the means of the seven behavioral factors). The step-wise criteria were to accept variables at significance level less than 5% and exclude variables of more than 10%. The ANOVA results of running this regression model indicated that all awareness factors were included in the model and that the model was accepted at level of significance = 5% and Durbin-Watson value = 1.587.

Similar procedures was applied to the perception factors and the model was also accepted, however, at a more confident level of significance = 3% and Durbin-Watson value = 1.661. All perception variables were included as well.

Findings and conclusion
From the above analysis, one can conclude that the awareness factors have a causal relationship on the positive behavior of employees and managers toward computer security in organizations. It was found that perception factors have even stronger causal

Top

relationship with behavioral factors of the computer security in the organizations. The incremental difference between the perception factors and the awareness factors are small which implies that policy makers need to pay almost symmetrical attention to both the awareness and perception factors. These results were not surprising and came with coherence finding of other researches.[35] However, it is advised that IT policy makers need to differentiate between the nature and implication of the perception aspects and the awareness aspects to be able to design sound computer security policy.

It is recommended to carefully construct and enhance a concise security policy that covers employee access, authorization and responsibility. This security policy must be easily understood by employees at all levels. Furthermore, it is highly recommended to create two versions of the policy. One version is distributed for the non-technical staff users and a more technical version for the information system (IS) staff. The security policy should have upper management approval and be enforced with lower management supervision. Management is responsible for directing and controlling an organization's operations and establishing, communicating, and monitoring policies and procedures. In the same way, IT staff should undergo extensive and ongoing security awareness programs through newsletters, training sessions, annual reviews, seminars and surveys. Perception and awareness of computer security issues conduct should be considered even in employee evaluation and promotion. Managers and employees alike need to know that computer security software such as anti-virus programs, cameras, door locks and similar technologies will not be effective if employee and manager's perception and awareness of computer security is not up to standards.

It was clearly stated in the report the importance of the ethics in the organizational environment. So, the most important consideration is to hire and retain honest people. The company should consistently recognize and publicly reward honesty. A high standard of integrity accompanied by a policy of recognition and rewards will reduce the temptation to commit fraud.

[35] (Casabona and Yu, P22), (Wright, P58), (Paroby and Barrett, P 36).

List of References:

Casabona, Patrick and Yu, Songmei "Computer Fraud: Financial And Ethical Implications" Review Of Business. Fall 1998

Germain, Ellen "Guarding Against Internet Intruders" Management Science February 1995

Graham , Paul and Catlett, Jason "Face Off: Are Filters More Effective Than Laws In Stopping Spam?" Network World. May 2003

Hannaford, Craig S. "Can Computer Security Really Make A Difference?" Managerial Auditing Journal. 1995

Harowitz, Sherry L "Security's changing future" Security Management. January 1997

Hochhauser, Mark "How well can your members read your online privacy policy?" Managed Care Quarterly. Summer 2002

Johnson, Deborah G and Mulvey, John M "Accountability and computer decision systems" Association for Computing Machinery. December 1995

Lock, Karen D , Conger, Sue "Ownership, privacy and monitoring in the workplace: A debate on technology and ethics" Journal of Business Ethics. April 1998

Milberg, Sandra J, Burke, Sandra J, Smith, H Jeff and Kallman, Ernest A "Values, personal information privacy, and regulatory approaches" Association for Computing Machinery. December 1995

Paroby ,Stephen M and Barrett, William J "Preventing Computer Fraud- A Message For Management" The CPA Journal November 1987

Schwartau, Winn "Cyber Ethics In The Workplace" Network World. January 2002

Scott, Robert W. "A Secure Business" Accounting Technology. April 2003

Simpson, Roy L "Security Threats Are Usually An Inside Job" Nursing Management. December 1996

Simpson, Roy L "What To Do Before Disaster Strikes" Nursing Management. November 2001

Smoyak, Shirley A. "Editorial: Computers and the World Wide Web--personal security and privacy protection" Journal of Psychosocial Nursing & Mental Health Services. October 2002

Stair, R. M. and Reynolds, W. G "Principles of information systems 5th ed." Course Technology. 2001

Tuttle, Brad, Harrell,Adrian and Harrison, Paul “Moral hazard, ethical considerations, and the decision to implement an information system” Journal of Management Information Systems. Spring 1997

Waldo, Billie Heister “Managing data security: Developing a plan to protect patient data” Nursing Economics. January/ February 1999

Weisband, Suzanne P, Reinig, Bruce A. “Managing user perceptions of email privacy” Association for Computing Machinery December 1995

Weiss, W H “The Need For Ethical Behavior” Supervision. December 1997

Whitman, Michael and Mattord, Herbert “Principle Of Information Security” Thomson Learning. December 2002

Wright, Phillip C “Computer Security In Large Corporations: Attitudes And Practices Of Ceos” Management Decision. 1993

Appendix (A)

Awareness factors
. Employees in our department are personally involved in the process of designing the computer security plans
2. I can discuss the general concept of our computer security issues with some confidence
3. Our management fully understand and support security policies
4. Security policies can be easily understood by employees at all levels
5. Employees in our department usually know and use new computer security applications before other people do
6. Employees in our department personally review and/or approve policies that guide the implementation of our computer security program
7. Employees in our department are well informed about computer security procedures
8. Our department dedicates a sufficient amount of its resources to computer security issues
9. Employees in my department fully understand the specific actions that will be taken if the computer security policies are not followed
10. Everybody is responsible for security not only the IS department
Perception factors
. Computer crimes threats to business have been exaggerated
. Computer security benefits everyone
. We are not doing enough in the company to protect the computer
. Too much money is wasted on computer security
. In my opinion, IS in my organization is well- protected
. Governments should make laws regarding computer security for companies
. In my organization, computer security is included in the strategic planning process
. My organization has a well-designed computer security system
. Each management unit recognize the computer security as a competitive advantage
0. If we continue with our present security, then the business will have to deal with serious problems in the future
Computer security is seen as being closely tied to the degree of success or failure of our department
Planning for computer security is seen as high-priority responsibility in our organization
In my opinion, IS in my organization good security practices
Existing procedures and guidelines hinder individuals in our department from trying out new ideas
Behavior factors
. Computer security responsibilities in our department are pushed down to the lowest possible organizational level
2. A computer security risk analysis had been conducted within the past three years
3. Ethics and good management practices will reduce computer crimes and the intentions to commit such crimes
4. In my organization we have a comprehensive ethics policy
5. My organization has a culture that is security conscious
6. In my organization there is a well-established security contingency plan

٦. If a new computer security application is available in the market, our department would be interested enough to order it immediately

In order to help us classify you and other respondents with similar evaluations of the product, we kindly request you to provide the following demographic information:

What is your age?
[ ] Below 25 years. [ ] 26 - 35 years. [ ] 36 - 45 years
[ ] 46 - 50 years. [ ] Over 50 years

What is your nationality?
[ ] Saudi [ ] Expatriate

What is the highest education level you have attained?
[ ] Elementary [ ] High school [ ] Diploma
[ ] University degree [ ] Master [ ] PhD

What is your monthly income?
[ ] Less than SR 3,000 [ ] SR 3,000- SR 5,999 [ ] SR 6,000- SR 9,999
[ ] SR 10,000 - SR 14,999 [ ] SR 15,000 - SR 20,000 [ ] Over SR 20,000

What is your area of specialty (i.e. major)?
[ ]

What is your management level?
[ ] top [ ] middle [ ] operational

How many years did you work in this organization?
[ ] 1 – 3 years [ ] 4 – 6 years. [ ] 7 - 10 years
[ ] 11 - 15 years. [ ] 16 - 20 years. [ ] Over 20 years

How many years did you work in this current job?
[ ] 1 – 3 years [ ] 4 – 6 years. [ ] 7 - 10 years
[ ] 11 - 15 years. [ ] 16 - 20 years. [ ] Over 20 years