Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication
of the Informing Science Institute
InformingScience.org

IJIKM.org

Volume 15, 2020

The Effect of Rational Based Beliefs and Awareness on Employee Compliance with Information Security Procedures: A Case Study of a Financial Corporation in Israel

Golan Carmi	Jerusalem College of Technology, Jerusalem, Israel	carmi@jct.ac.il
Dan Bouhnik*	Jerusalem College of Technology, Jerusalem, Israel	bouhnik@jct.ac.il

* Corresponding author

Abstract

Aim/Purpose: This paper examines the behavior of financial firm employees with regard to information security procedures instituted within their organization. Furthermore, the effect of information security awareness and its importance within a firm is explored.

Background: The study focuses on employees' attitude toward compliance with information security policies (ISP), combined with various norms and personal abilities.

Methodology: A self-reported questionnaire was distributed among 202 employees of a large financial Corporation

Contribution: As far as we know, this is the first paper to thoroughly explore employees' awareness of information system procedures, among financial organizations in Israel, and also the first to develop operative recommendations for these organizations aimed at increasing ISP compliance behavior. The main contribution of this study is that it investigates compliance with information security practices among employees of a defined financial corporation operating under rigid regulatory governance, confidentiality and privacy of data, and stringent requirements for compliance with information security procedures.

Findings: Our results indicate that employees' attitudes, normative beliefs and personal capabilities to comply with firm's ISP, have positive effects on the firm's ISP compliance. Also, employees' general awareness of IS, as well as awareness to ISP within the firm, positively affect employees' ISP compliance.

Accepting Editor Salah Kabanda │ Received: February 3, 2020 │ Revised: April 3, April 17, May 23, June 22, 2020 │ Accepted: June 28, 2020.

Cite as: Carmi, G., & Bouhnik, D. (2020). The effect of rational based beliefs and awareness on employee compliance with information security procedures: A case study of a financial corporation in Israel. *Interdisciplinary Journal of Information, Knowledge, and Management, 15,* 109-125. https://doi.org/10.28945/4596

Recommendations for Practitioners This study can help information security managers identify the motivating factors for employee behavior to maintain information security procedures, properly channel information security resources, and manage appropriate information security behavior.

Recommendations for Researchers Researchers can see that corporate rewards and sanctions have significant effects on employee security behavior, but other motivational factors also reinforce the ISP’s compliance behavior. Distinguishing between types of corporations and organizations is essential to understanding employee compliance with information security procedures.

Impact on Society This study offers another level of understanding of employee behavior with regard to information security in organizations and comprises a significant contribution to the growing knowledge in this area. The research results form an important basis for IS policymakers, culture designers, managers, and those directly responsible for IS in the organization.

Future Research Future work should sample employees from another type of corporation from other fields and should apply qualitative analysis to explore other aspects of behavioral patterns related to the subject matter.

Keywords information security behavior, information security awareness, information security management, information security policy, employee compliance financial corporation

INTRODUCTION

Information security (IS) is defined as the terms, methods, technical, and administrative means employed to protect information assets against unauthorized—intentional or otherwise—acquisition damage, exposure, manipulation, change, loss or use (Acquisti et al., 2006). A broad term encompassing two basic intertwining foundations: information systems security and computer security. Accelerated technological development, specifically the Internet, blurs the boundaries between the private and public domains, thus changing the perception of information security. Moreover, generating new threats and challenges for the users and the Internet companies (Eckersley, 2010).

However, information security is not limited to technical or technological matters. In order to ensure information security, one must not only manage the technical aspect or the security procedure mechanism, but also the human aspect, which must be treated on the same level. The best information security cannot protect the information without the cooperation of the individuals involved, especially as they are, at times, the weakest link in information security (Trepte et al., 2015). In order to bring about this cooperation, one must create among these individuals the awareness of the threat to the wholeness and the privacy of the information and of the necessity to take active steps in order to protect it. Research has shown that by elevating the level of awareness to information security threats it is possible to increase information security and sense of privacy (Weinberger et al., 2017; Weinberger & Bouhnik, 2019).

Organizations may write binder instructions and establish information security policies, but this does not guarantee that employees will actually follow the procedures. It is therefore necessary to understand the factors that motivate employees to comply with information security procedures, and thus reduce risky behaviors.

In the research literature in the field of information security, we did not find empirical studies that directly examined employee compliance with information security practices and information security awareness in regulated organizations such as financial corporations. While prior studies (Bulgurcu et al., 2010; Harris et al., 2014; Herath & Rao, 2009b; Schlienger & Teufel, 2002) have looked at employee information security behaviors in wide-ranging organizations, this research is a case study in a financial corporation. Also, due to the characteristics of the corporation, the study surveyed employees who work in a closely monitored environment that is unique in terms of complying with information security procedures.

It is well known, that financial organizations all over the world, are highly regulated and monitored closely by government institutions regarding information security procedures and processes. Therefore, our goal in this study is to expand the knowledge base of motivational factors of employees to comply with the information security procedures in their organization. The study examines the behavior of employee's in a financial corporation with regard to information security procedures. The study also inspects the employees' awareness of information system procedures in the organization, and explores to what extent promotion of this awareness is essential and necessary to ensure information security. To achieve this goal, we scrutinized information security systems in financial organizations, where the issue is considered a high priority value and the need for compliance among the employees is substantial.

LITERATURE REVIEW

INFORMATION SECURITY

Information systems security comprises actions aimed at protecting computer systems against threats, unauthorized access and use, disruption, distortion and destruction. In today's companies, almost all of these actions are dependent upon technological tools. Many databases serve individuals, companies, even countries, and these include both personal and business information; thus, the protection against penetration and damage becomes critical.

A number of studies have discussed many of the aspects regarding information security (Aydin & Chouseinoglou, 2013; Bouhnik & Deshen, 2014; Carmi & Bouhnik, 2016; Cavusoglu et al., 2004; Talib et al., 2010). Some focused on the importance of information security economic aspects (e.g., Cavusoglu et al., 2004), while others highlighted its significance for every company and organization, public and private as one, regardless of the importance of the information, the level of risk or its sensitivity (e.g., Carmi & Bouhnik, 2016).

Information security failures can lead to the disruption of business and to the violation of confidentiality and privacy, damaging the ongoing activity and reputation of the organization, as well as causing financial harm brought about by fines and regulation violations. Currently, organizations recognize the importance of securing their infrastructures through which their strategic information may be transferred. In this era, information security has become an integral part, sometimes even the spearhead, of business (Itradat et al., 2014).

The design and development of information security procedures has attracted research attention. Stahl et al. (2008) presented an information security management system (ISMS) that relates to all aspects of the corporation involved in the creation and maintenance of a secure information environment that contributes to savings in information management. The ISMS also aids in the evaluation of the information security level within the organization. The system comprises various aspects, such as policies, standards, instructions, technology, human issues, legal and ethical issues.

Several scholars have discussed the connection between information security and management. Björck (2005) claimed that proper management creates an atmosphere of information security in the corporation and that without clear guidelines the corporation would not succeed adequately in integrating information security procedures. Albrechtsen (2008) argued that the quality of the management affects employees' awareness, motivation, and behavior, thus requiring the commitment of management levels to the maintenance of information security within the organization. Research has also indicated that one of the most tested methods of the internalization of information security in organizations is the *carrot and stick* method, punishing and rewarding accordingly (Puhakainen & Siponen, 2010).

Im and Baskerville (2005) differentiated between deliberate security threats and human error. Their findings indicated that a large percentage of security problems result from human error, so protection against malicious attacks is not enough. Protection against human error has been, and remains, one of the significant issues regarding information security (see Figure 1 for a summary of types of threats).

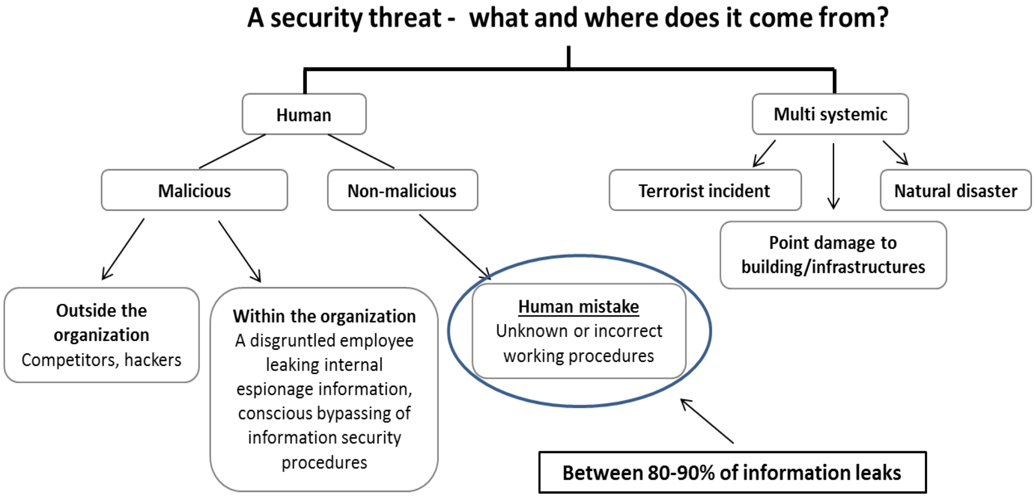
A security threat - what and where does it come from?
Human
Multi systemic
Malicious
Non-malicious
Terrorist incident
Natural disaster
Point damage to building/infrastructures
Outside the organization
Competitors, hackers
Within the organization
A disgruntled employee leaking internal espionage information, conscious bypassing of information security procedures
Human mistake
Unknown or incorrect working procedures
Between 80-90% of information leaks

Figure 1: Security threat sources involving human and non-human factors (Im & Baskerville, 2005).

INFORMATION SECURITY BEHAVIORS

Many studies have highlighted the importance of the human aspect of information security. Goh (2003) cited security expert Ira Winkler: "From a security aspect, the people within the corporation are the company's greatest concern; number two is not even close" (p. 37). Other researchers, such as Kotzias et al. (2016) and Fagerström (2013) took a similar approach and emphasized the dangers stemming from the members of the corporation itself. These employees may comprise a threat as a consequence of authorizations they have received and procedures for which they are responsible, which they misuse, intentionally or otherwise.

Herath and Rao (2009a) added that management's approach toward the demand for proper information security behavior directly affects employees' attitude. Fagerström (2013) recommended procedures for establishing such an environment. Wang et al. (2018) also mention improvement of social contacts via organizational bodies (commitment, involvement, norms) as an effective tool for preventing misuse of computers.

Herath and Rao (2009b) found that motivation for adhering to information security procedures is based on intimidation by punishment. The intimidation theory maintains that as the certainty of punishment rises, the level of the threats of the actual punitive measures rises. Pahnila et al. (2007) also investigate motivational factors in order to explain employee compliance behavior. They found that sanctions and rewards did not influence the intention of employees to comply or actual compliance, and that information security may interfere with the primary goals of organizations. Accordingly, Tyler and Blader (2005) claim punishments and rewards are external motivations, but it is well known that employee's intrinsic values provide internal motivation to follow regulations and procedures.

D'Arcy et al. (2009) reveal a positive effect of intimidation on information security, but found that the certainty of punishment had no real effect, with the level of discouragement reliant upon the individuals' own ethical standards. Wang et al. (2018) also speak of the "stick & carrot" method. They are of the opinion that in certain situations intimidation has a positive effect on compliance and at times rewards are more beneficial, depending on the general environment within the organization and the employees feeling of commitment.

Indeed, improper information security behavior can derive from several qualities of the individual: bitterness, malicious intent, lack of knowledge, negligence, indifference, etc. Some of these problems may be resolved by the creation of awareness. Employees who are aware of the devastating consequences information security deficiencies can cause can be less indifferent and more conscious of security breaches at their place of employment (Chen & Li, 2019).

Information Security Awareness

Lack of attentiveness is a critical factor in information security. While formal information security procedures have a great effect on employee behavior, lapsed procedures or procedures which do not promote awareness have no impact on employee behavior. One of the effective ways to combat negligence and carelessness is the generation of awareness among the users. Establishing awareness of security threats will help the employees understand the gravity of the threats and improve their compliance to security procedures. A team which is aware of the security concerns can prevent incidents. Gundu and Flowerday (2013) and Bulgurcu et al. (2010) have all indicated the workers' crucial role in the maintenance of information security.

Puhakainen's review (2006) tapping over 300 articles on information security revealed that the greatest danger to organizations with regard to information security is the lack of cooperation by members of the organization. The most advanced security measures will not protect the information without the organizations' members' cooperation. Moreover, the most essential element upon which this cooperation is based is the awareness of all the members of the group and their willingness to adhere to the information security instructions.

Puhakainen and Siponen (2010) suggested a theory that improves information security awareness training. McIlwraith (2006) in his book *Information security and employee behavior* identified four aspects in awareness planning: technological infrastructure, regulations and standards, ensuring the employee has the capabilities to carry out his job, and the systems and the environment in which the employee does so.

Schlienger and Teufel (2002) as well as Alfawaz (2015) indicated the significance of creating an organizational culture that would encourage information security and its centrality to the organization. Research has clearly indicated that information security plans cannot adequately be implemented without an operational plan for heightening the awareness of the employees of information security. Internalizing information security is a process which demands a cultural change for most employees. Organizations' information security programs must provide a high level of understanding of security threats that can result in damage and loss of data. From a management point of view, the programs must be composed of two main elements: awareness, whose purpose is to arouse the workers, and teaching and instilling the necessary expertise (Harris et al., 2014).

In the current study, we scrutinized the general awareness of the employees to the various security issues, employees' recognition of the importance of information security to the corporation in which they are employed, and acquaintance with the company's information security procedures. Our attempt to understand the factors affecting employee compliance with information security demands is based on Bulgurcu et al.'s (2010) study, which grounded its research on the issue on the theory of planned behavior (TPB), which sees behavioral intention as an indication of an individual's willingness to behave in a certain way. The theory embraces three major constructs: attitude, subjective norms, and the perception of behavior control in the context of precedents, which motivate the employees' intention to comply with information security policies (ISP). To this model they added the basis for cognitive beliefs, which is rooted in the rational choice theory (RCT), as factors affecting attitudes. Finally, they studied the role of awareness on employees' intentions and its effect on how they relate to the demands made upon them. In their study, employees' intention to comply with ISP policies served as the dependent variable. In this paper, we expanded their research and examined whether the factors influencing employees' intents affect their actual behavior. We adopted these theories as they are highly recognized in this field. The adoption of both of the two cited theories as the basis for our research derives from their complementarity and their composition of elements—attitude, subjective norms, the perception of behavior control and rationalism—which correspond theoretically to the research and have great influence on behavior in practice. These two behavioral theories are presented in the next section.

THE THEORY OF PLANNED BEHAVIOR (TPB)

Fishbein and Ajzen (1975) noted that the main factor in actual behavior is intent. Intent indicates the amount of effort one is willing to invest in order to carry out a specific action. The more serious the intent, the higher the chance the action will be performed. As a rule, the more positive the stand, the more subjective the norm and the higher the behavior control seems; thus, the stronger the behavioral intention, the likelihood of manifesting the behavior is more significant. The theory includes three main factors which affect behavioral intentions:

1. Attitude: the degree in which the individual evaluates a specific behavior positively or negatively.
2. Subjective norms: a social factor, reflecting the perception of social pressure regarding a certain behavior.
3. The perception of behavior control: how easy or challenging a behavior is perceived to be.

According to TPB, various beliefs affect the three factors: (1) beliefs regarding the potential positive or negative results, which affect the attitude; (2) beliefs regarding normative behavior and the willingness to follow suit, which affect subjective norms; (3) beliefs regarding the difficulty or facility of a behavior, which affect one's perception of behavior control. Furthermore, other personal background variables, such as: demographics, experience, and knowledge affect all three factors. Figure 2 presents the components of the TPB theory.

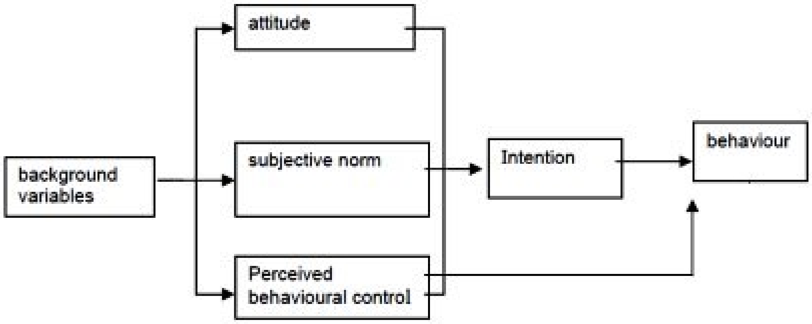

Figure 2: The theory of planned behavior - Organizational Behavior and Human Decision Processes (Ajzen, 1991).

With regard to information security, we assume that employee awareness, perceived as a background factor, leads to the formation of consequence beliefs tied to obedient behavior.

THE RATIONAL CHOICE THEORY (RCT)

Rational choice theory is an economics approach, which proposes a theoretical explanation for how people make decisions when faced with several alternatives. According to RCT, the individuals determines how they will act by balancing the costs and the benefits of the various possibilities. According to this approach, people always calculate the costs and the benefits which will result from a specific action or behaviour. The total evaluation of the costs and benefits regarding a course of action is formed by the individual's perception of the potential outcome of that action. Finally, the individual examines all the comprehensive evaluations of all possible courses of action in order to assert which is the best alternative which “maximizes” his gain (Scott, 2000).

RESEARCH GOALS

The purpose of this research is to inspect the ISP compliance behavior of employees in a financial corporation that is under IS supervision and regulation, while identifying the factors which affect employee behavior, and examining the associations between the examined factors and actual compliance behavior. Our goal is to determine if these factors have a positive or a negative effect on employee ISP behavior. We will also explore the relation between IS awareness among the employees and their actual behavior in this regard.

Based on the theory of planned behavior and the rational choice theory, this study explores whether employees’ intention to comply with ISP is affected by attitude, normative beliefs, and personal capacity to do so. *Attitude* refers to the employees’ attitude toward compliance and includes the following elements: 1) the employees’ evaluation of the benefits of observing ISP (rewards, the safety of the corporations’ systems); 2) the cost of compliance (work disruption and lower productivity); 3) the cost of noncompliance (sanctions, putting corporations’ systems in danger). *Normative beliefs* refer to social pressure from managers and colleagues to comply with ISP. *Personal capabilities* refer to employee knowledge, capabilities, and talents. The study will also explore how awareness of the IS policies and requirements affects the employees’ attitude and their evaluation of the benefit of observing ISP.

Accordingly, eight research hypotheses were formulated:

1) Employees’ attitude toward ISP compliance will have a positive effect on their ISP compliance (H1).
2) Employees’ normative beliefs regarding ISP compliance will have a positive effect on their ISP compliance. (H2)
3) Employees’ personal capabilities to observe ISP will have a positive effect on their ISP compliance. (H3)
4) Employees’ general evaluation of the benefits of ISP compliance will have positive effect ISP compliance within the organization. (H4)
5) Employees’ general evaluation of the costs of ISP compliance will have a negative effect on ISP compliance within the organization. (H5)
6) Employees’ general evaluation of the costs of ISP noncompliance will have a positive effect on ISP compliance within the organization. (H6)
7) Employees’ general awareness of IS and ISP compliance will have a positive effect on ISP compliance within the organization. (H7)
8) Employees’ awareness of the ISP within the corporation will have a positive effect on ISP compliance within the organization. (H8)

In accordance with TPB, we first explore the employees’ attitude toward compliance with ISP. We will also check if the employees’ normative beliefs, that their behavior—compliance or non-compliance—leads to specific results (costs and benefits) determine their attitude toward behavioral compliance.

According to RCT, we define normative beliefs as the beliefs regarding the general evaluation of the consequences of compliance or non-compliance. In other words, the result of ISP compliance, the cost of compliance and the result of non-compliance with procedures comprise the general evaluation of compliance consequences.

In our study, we will focus on the first component of the TPB theory—attitude–and on the various motives which bring about positive or negative attitudes toward compliance with ISP. According to TPB theory, employees' attitude toward a certain behavior is tied to their beliefs regarding the results of their actions. RCT enables identification of the beliefs and the consequences of alternative courses of action; with regard to our study, the courses of action refer to compliance or non-compliance. Compliance with procedures is an active behavior which entails a certain amount of effort on the employees' part. Therefore, when making their decision, employees consider the amount of effort required to comply. In light of this, the beliefs comprising the total evaluation of the consequences include three factors:

1. Positive consequences of compliance.
2. Negative consequences of compliance.
3. Negative consequences of non-compliance.

According to RCT, the individual examines all the comprehensive evaluations of all the possible courses of action in order to assert which is the optimal alternative which maximizes his gain. Regarding our study, employees are expected to examine the anticipated cost and gain in case of compliance and non-compliance to ISP, and choose the alternative which is in their best interest. Based on the TPB theory, the assumption is that the employees' beliefs regarding predicted consequences and results will affect his attitude toward ISP compliance.

Bulgurcu et al. (2010) defined the seven consequence beliefs which provide the basis for employees' beliefs, including the consequences of obedient ISP behavior.

1. Sanctions –one of the consequence beliefs tied to obedience because it is generally accepted that individuals will obey threats based on sanctions; furthermore, punishment, as a dissuasion tool, is accepted among policy makers and the general public.
2. Rewards –an essential tool in encouraging desirable behavior.
3. Internal cost – guilt, embarrassment, shame and stress.
4. Significant benefit – satisfaction, achievement.
5. Function prevention – If an employee complies with ISP, his job performance may suffer.
6. Source damage – If an employee chooses not to comply with ISP, the organizations' systems become vulnerable to information security threats; therefore, damage is a crucial element which derives from non-compliance.
7. Resource safety – If employees comply with ISP, they contribute to the protection of the organization's information sources and its technology, thus contributing a crucial element which derives from compliance.

These seven consequence beliefs will serve as the basis for the correlating beliefs regarding the evaluation of the consequences of compliance and we will attribute them to the three compliance benefit categories (significant benefit, resource safety, rewards) as well as cost of compliance (setback in work progress) and cost of non-compliance (sanctions, internal cost, source damage).

Figure 3 depicts the model of this research study.

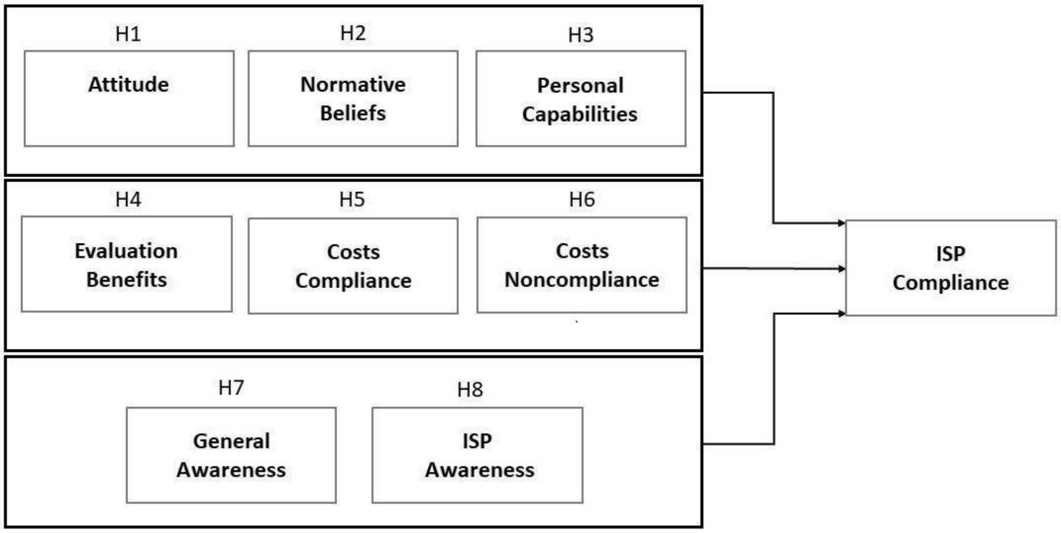

Figure 3: The research model

METHODS

SAMPLE POPULATION

We believed that the best approach to this study would be a quantitative approach, as we wished to collect a large amount of data in order to obtain a clear picture of the situation in the firm. Hence, data was collected by a self-report questionnaire, distributed among employees of a large financial corporation (2000 employees) via the corporation's internal email system. The firm has eleven departments and we distributed twenty-five questionnaires to each. Out of 275 distributed questionnaires, 202 were completed (73.5%). Participants represented all positions in the corporation, professional as well as administrative. It was explained to the participants that the questionnaires are anonymous and all information collected will be used for research purposes only, therefore we believed that they would be honest with their reports. The corporation's information security department comprises six employees charged with the corporation's information security issues, including both technological and publicity aspects. The corporation invests considerable resources to increase awareness and improve information security behavior, as a part of regulatory demands. These regulations aim to maintain, encourage, and establish proper information security behavior among employees at all levels. The efforts include advertisement of instructions, employee training, educational computer training programs, periodical emails for refreshing guidelines, and discussion of specific security occurrences, such as cyber-attacks.

Of the 202 participants, 54% were female; 62% between the ages of 26-45 (33% ages 26-35, 29% ages 36-45); eleven percent of the participants were employed by the corporation for less than a year, 46% for 2-5 years, 31% for 6-10 years, and 12% for over 10 years. The participants' distribution among all the corporations' departments reflects the relative size of the departments.

DATA COLLECTION METHOD

The questionnaire was based on a questionnaire developed and validated by Bulgurcu et al. (2010), with a few minor changes and local adaptations. The questionnaire explored employees' behavior with regard to the organization's information security procedures, to what degree they heed the organization's procedures and directives, and to what degree are they aware of information security in general, and within the corporation specifically. Despite the questionnaire's initial credibility, it was submitted to two colleagues who reviewed the statements reflecting TPB and RCT. They also confirmed that all the behavior patterns received fair representation in the questionnaire. The statements were revised in accordance with their impressions and were analyzed in a pre-study (*N* = 18). Following the results, a number of statements underwent revisions. Questionnaire validation was performed using content validity and face validity procedures.

DATA ANALYSIS RESULTS

Almost half (48%) of the participants reported their being very aware of general security issues, and 38% reported having extremely high awareness. Regarding awareness of security issues within the corporation, 42% reported that they very much understood the importance and the dangers relating to information security in the organization; 80% reported their having considerable understanding regarding ISP, and 75% stated that they make an effort to comply with the ISP related to their positions to a large extent, in order to protect the corporation's information and technology; 76% reported that they protect information privacy to a very high extent.

Study index credibility was analyzed as internal consistency by Cronbach'sα. The average of the items belonging to each index was calculated, including standard deviations and the average correlation among the items. Table 1 indicates a medium to high credibility of all the questionnaire's indices among the items, reflecting adequate to high internal validity among the study's indices.

Table 1: Findings of Index Credibility of Internal Consistency (Cronbach'sα), Average, Standard Deviation and Average Correlation among Index Items

Index	Average	STD	Range	Average Correlation among Items	Alpha Credibility	Number of Items in Index
Positive Attitude toward ISP compliance	4.159	1.288	1.741	0.211	0.673	5
Normative beliefs regarding ISP compliance	4.345	1.396	2.213	0.514	0.800	4
Employee's capability to observe ISP	4.028	1.547	1.213	0.735	0.918	4
Total evaluation of ISP compliance benefits	4.316	1.357	0.632	0.447	0.680	4
Total evaluation of ISP compliance cost	2.949	1.419	0.777	0.576	0.923	5
Total evaluation of ISP noncompliance cost	4.405	1.269	0.624	0.606	0.820	4
General awareness of IS	4.936	1.176	0.193	0.848	0.943	4
Awareness of organization's ISP	4.966	1.137	0.173	0.801	0.952	5

Linear regression was conducted in the stepwise method for anticipating the level of ISP compliance, with the dependent variable being ISP compliance and the non-dependent variables being the six variables. This was carried out to ascertain whether employee's attitude, their normative beliefs, and their personal capabilities regarding company ISP have a positive effect on their ISP compliance. Also, the linear regression would help determine if the total evaluation of ISP compliance benefits and the total evaluation of ISP non-compliance costs have positive effects and if total evaluation of ISP compliance cost has a negative effect on ISP compliance. Table 2 represents the results.

Table 2: β's Value for Employee's Attitude, Normative Beliefs and Personal Capabilities regarding Company ISP Variables

Variables	**ISP Compliance**				
	β	**SE**	**B**	**Adj. R²**	***F* Value**
Positive attitude toward ISP compliance	1.092	0.061	0.786***	0.617	322.859***
Normative beliefs regarding ISP compliance	0.719	0.043	0.763***	0.582	278.208***
Employee's capability to observe ISP	0.756	0.054	0.792***	0.623	332.749***
Total evaluation of ISP compliance benefits	0.687	0.050	0.700***	0.490	192.066***
Total evaluation of ISP compliance cost	-0.598	0.051	-0.642***	0.412	140.284***
Total evaluation of ISP noncompliance cost	0.764	0.041	0.799***	0.638	353.104***

***p < .05, ** p< .01, ***p < .001**

Table 2 shows that an increase of one unit in positive attitude toward ISP compliance generates a significant increase of 1,092 units in ISP compliance (*t* =17.968*, p* < .001). The relation between attitude and compliance is positive, significant, and high *(r* =763., *p* < .001). In other words, as the positive attitude toward compliance rises, ISP compliance rises. In addition, a positive attitude regarding compliance can explain 61.7% of the variance of ISP compliance.

Furthermore, every increase of one unit of normative beliefs regarding compliance generates a significant increase of 0.719 units in ISP compliance (*t =16.680, p* < .001). The relation between normative beliefs regarding compliance and ISP compliance is positive, significant, and high *(p* <.001*. r* =76*).* In other words, as the normative behavior beliefs regarding compliance rises, ISP compliance behavior rises. Normative beliefs regarding compliance can explain 58.2% of the variance of ISP compliance behavior. Additionally, every increase of one unit of compliance capability generates a significant increase of 0.756 units in ISP compliance behavior (*t* =17.580*, p*< .001). The relation between capability and ISP compliance is positive, significant, and high (*p* < .000, r = .792). In other words, as the employee's ISP compliance capability rises, so rises ISP compliance. We learn from the table that compliance capability can explain 62.3% of the variance of ISP compliance behavior.

Table 2 also shows that every increase of one unit of the total evaluation of ISP compliance benefits generates a significant increase of 0.687 units in ISP compliance behavior (*t* =13.859, *p* < .001). The relation between the total evaluation of ISP compliance benefits and ISP compliance is positive, significant, and med-high *(p* < .001, r =.700). In other words, as the total evaluation of ISP compliance benefits rises, thus does rise ISP compliance. We learn from the table that total evaluation of ISP compliance benefits can explain 49% of the variance of ISP compliance. Furthermore, every increase of one unit of the total evaluation of ISP compliance cost generates a significant decrease of 0.598 units in ISP compliance *(t* =11.844, *p* <.001). The relation between the total evaluation of ISP compliance cost and ISP compliance is negative, significant, and med (*p*<.001, *r* = .642). In other words, as the total evaluation of ISP compliance cost rises, so does ISP compliance decline, and as the total evaluation of ISP compliance cost decreases, so does ISP compliance rise. We learn from Table 2 that total evaluation of ISP compliance cost can explain 41.2% of the variance of ISP compliance behavior. Additionally, every increase of one unit of the total evaluation of ISP non-compliance cost generates a significant increase of 0.764 units in ISP compliance (*t* =18.791, *p* < .001). The relation between the total evaluation of ISP non-compliance cost and ISP compliance is positive, significant, and high *(p* < .000, *r* = .799). In other words, as the total evaluation of ISP non-compliance cost rises, so does ISP compliance behavior rise? We learn from the table that total evaluation of ISP non-compliance cost can explain 63.8% of the variance of ISP compliance.

In order to ascertain if the employee's general awareness of IS, and their awareness of the organization's ISP have a positive effect on ISP compliance, a linear regression was conducted in the step method for anticipating the level of ISP compliance, with the dependent variable being ISP compliance and the two non-dependent variables being general awareness of IS and awareness of the organization's ISP (see Table 3).

Table 3: β's Value for Awareness regarding ISP Variables

Variables	**ISP Compliance**				
	β	**SE**	**B**	**Adj. R²**	***F* Value**
General awareness of ISP	0.737	0.041	0.789***	0.622	328.975***
Awareness of organization's ISP	0.832	0.039	0.834***	0.695	455.708***

*****p < .001**

Table 3 shows that an increase of one unit in general awareness of IS generates a significant increase of 0.737 units in ISP compliance (t = 18.138, p < .001). The relation between general awareness of IS and ISP compliance is positive, significant, and high (r =789. , p < .001). In other words, as the general awareness of IS rises, so rises ISP compliance. We learn from the table that a general awareness of IS can explain 62.2% of the variance of ISP compliance. Furthermore, an increase of one unit of ISP awareness generates a significant increase of 0.832 units in ISP compliance (t =21.347, p < .001). The relation between ISP awareness and ISP compliance is positive, significant and high *(r* =. 834*,* p< .001). In other words, as the ISP awareness rises, so does ISP compliance. We learn from the table that ISP awareness can explain 69.5 % of the variance of ISP compliance.

Analysis of the employee's demographics did not reveal significant associations between ISP compliance behavior and gender, age, or department affiliation. However, regarding pay grade, an indication of seniority and socio-economic status, we found that the higher the pay grade, the higher the general awareness of IS and actual ISP compliance. With regard to seniority in the corporation, new employees (under two years) and senior employees (over 10 years) tended to be more compliant with ISP than were employees with 2-10 years of seniority.

The study's findings indicate a significant relation between the independent variables and the dependent variable – ISP compliance. Employees' attitudes, normative beliefs and personal capabilities to comply with corporation's ISP, have positive effects on the corporation's ISP compliance. Moreover, the total evaluation of ISP compliance benefits (substantial benefits, resource safety and compensation) positively affects ISP compliance within the corporation. Total evaluation of ISP compliance cost (hindrance of work assignments) has a negative effect on the corporation's ISP compliance and vice-a-versa. Total evaluation of ISP non-compliance costs (sanctions, internal costs and resource damage) positively affects ISP compliance within the corporation. Also, employees' general awareness of IS, as well as awareness to ISP within the corporation, positively affect employees' ISP compliance. Thus, the findings indicate statistical support for all eight of the research hypotheses, with all hypotheses confirmed.

DISCUSSION

In this study, we examined the level of awareness and the compliance behavior of employees regarding ISP in a large financial corporation. While professional literature has discussed the role and the importance of rewards and sanctions in the context of information security, the conclusions have not been definitive. This study establishes the substantial effect that both rewards and sanctions have on employee behavior with regard to ISP compliance.

The current findings clearly indicate a high level of compliance behavior and ISP compliance within the investigated corporation. Also, a high level of awareness was found among the corporation's employees regarding IS in general and specifically, with regard to the corporation's IS situation. These findings appear to match the stringent demands for IS in the investigated corporation and its heightened enforcement of regulation, as an integral part of their business activities in the finance arena. Additionally, the results indicate that the employees at all levels not only understand the immense importance of ISP implementation at both the personal and organizational levels, but also have a conscious awareness and have adopted active behaviors regarding all that relates to the protection of the information resources and the security of the information itself.

Moreover, the research results indicate that conceptions and personal beliefs of the employees significantly affect behavior regarding all that relates to compliance with ISP. Similar to other studies (Albrechtsen, 2008; Björck, 2005; Puhakainen & Siponen, 2010), our findings show a close association between ISP behavior and personal consequences—positive and negative—as an outcome of the actions which derive directly from the employees' manner of behavior. For instance, an anticipation of personal benefit increases the level of compliance, while imposing a personal cost as a result of non-compliance directly and positively affects compliance. In other words, the manner in which employees evaluate how compliance or non-compliance with IS procedures will affect the progress of his work assignments on the one hand and personal sanctions on the other hand, are parameters which greatly influence the level of actual compliance with the corporation's ISP. Appropriate awards may actually increase ISP compliance levels and cause employees who do not recognize the importance of information security to comply with ISP. While our findings are consistent with Bulgurcu et al.'s work (2010), Herath and Rao (2009b) and Wang et al. (2018) they seem incompatible with other studies that did not reveal substantial effects of enforcement and sanction policies regarding ISP compliance behavior (D'Arcy et al., 2009; Pahnila et al., 2007).

Another interesting finding is the relation between employee behavior and the security of the corporation's systems. Although it is clear that ISP compliance is meant, among other things, to help protect the corporation's information technologies, the results indicate that ensuring the safety of the information technology also affects employees' behavior and is an integral part of their behavior considerations. This behavior may be explained also as the desire to comply with ISP and also as an understanding of the importance of intactness and continuousness of the work environment, which is based mostly on information technology. This finding also supports previous studies (Kotzias et al., 2016).

Additionally, this study's findings are consistent with findings of others who have explored the relation between employee IS awareness and compliance behavior (Bulgurcu et al., 2010; Gundu & Flowerday, 2013). The distinction between general awareness and ISP organizational awareness illustrates the strong effect both types of awareness have on behavior and that employees having higher awareness levels are relatively more cautious and stricter about ISP compliance.

CONCLUSIONS AND RECOMMENDATIONS

From the sum of the findings, we can conclude that employee IS compliance level is a combined function of awareness and behavior. In order to achieve better information security results, organizations must invest time and resources on the development of IS awareness, as well as on information systems and resources. IS awareness is a valuable preliminary conscious basis for understanding the importance of information security behavior in general and the organizational need for protection of information, specifically.

Although many employees do not concern themselves with or invest time in activities which slow down or hinder their job performance and decrease their productivity, it must be emphasized to them that IS obedience is highly important and is part of their work time and commitment. In line with this, the workplace should allocate time to the employees for execution of these activities. An organizational culture which values IS, reflecting the importance of the issue among administrators and employees, along with a serious approach of the managers to the subject, all have a facilitative effect on ISP behavior.

The study found that attitude, beliefs and personal capabilities have a positive effect on employee ISP compliance. The general evaluation of the benefits and the cost of compliance or non-compliance have considerable effect on behavior, with the effect of the cost of compliance being as strong as the effects of the benefits of compliance and the cost of non-compliance. This result emphasizes the importance of these matters with regard to IS behavior. Furthermore, the study found that employees' general and organizational IS awareness also directly affect his compliance behavior. The study supports the theory of planned behavior and the rational choice theory -which may further explain employee behavior and their motivation to observe ISP. Thus, other behavioral theories may help explain a range of other behavioral characteristics of employees with regard to ISP.

In this light, we recommend that organizations strengthen their efforts to create awareness of IS among employees at all levels and ranges of seniority, presenting the issue in seminars and training programs in order to teach them the importance of IS and the practical consequences of related behaviors. Moreover, various aspects of awareness may be more effective in modifying beliefs and behavior, depending on their hierarchic level and position. Therefore, the programs should be constructed keeping in mind the characteristics of the employee groups they are targeting.

Organizations should put in place IS instructional and training programs. These programs should emphasize the employees' personal advantage of compliance with ISP, alongside the demands for retaining information resource security. This may be achieved by presenting the cost of non-compliance from the personal aspect of sanctions and personal cost, as well as the potential and concrete dangers which lie in wait as a result of disregarding procedures.

CONTRIBUTION AND LIMITATIONS

As far as we know, this is the first paper to thoroughly explore employees' awareness of information system procedures, among financial organizations in Israel and also the first to develop operative recommendations for these organizations aim to increase ISP compliance behavior. This study offers another level of understanding of employee behavior with regard to information security in organizations and comprises a significant contribution to the growing knowledge in this area. The research results form an important basis for IS policymakers, culture designers, managers, and those directly responsible for IS in the organization. The study indicates that rewards and sanctions have significant effects on employee behavior, but also other motivational factors reinforce ISP compliance behavior. Understanding the motivating factors of employees to comply with information security procedures, helps information security managers to identify the weakest human link, correctly channel information security resources and to conduct proper information security behavior.

Nevertheless, this study has some limitations. First, the findings are limited by the relatively small sample population that reflects the attitudes and behavioral patterns of Israeli employees of one financial institution. Therefore, future work should sample employees from other financial institutions and also intuitions from other fields (e.g., academic, infrastructure, government, etc.). Second, since our findings are based on the participants' self-reports regarding their attitudes and behavior it may be biased. Future work should apply qualitative analysis to explore other pillars of behavioral patterns related to the subject matter.

Summary

Organizations should ascribe much importance to the motives and personal factors which affect employee behavior. A clear message of the management, a strong organizational culture and guidelines on IS matters contribute to enhanced compliance behavior. A corporation which emphasizes the importance of ISP compliance at every level and in every position positively affects employee ISP compliance.

In summary, information security behavior is derived from the employees' attitude toward IS, to the whole of his normative beliefs and his personal capabilities to execute the organizational demands of his position. A combination of two components, awareness and behavior, creates a strong, valid mechanism which enhances the level of ISP compliance on the one hand, and decreases the level of ISP non-compliance on the other. Emphasizing and developing both components of the mechanism strengthen the ring of security surrounding the organization's information systems.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *Proceedings of the 27th International Conference on Information Systems (ICIS)* (pp. 1563-1580). Milwaukee, WI: Association for Information Systems. http://aisel.aisnet.org/icis2006/94

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211. https://www.dphu.org/uploads/attachements/books/books_4931_0.pdf

Albrechtsen, E. (2008). *Friend or foe? Information security management of employees* [Unpublished PhD Thesis.] Norwegian University of Science and Technology (NTNU). http://hdl.handle.net/11250/265659

Alfawaz, S. M. (2015). *Information security management: A case study of an information security culture* [Unpublished PhD Dissertation]. Queensland University of Technology. https://eprints.qut.edu.au/41777/1/Salahuddin_Alfawaz_Thesis.pdf

Aydin, O. M., & Chouseinoglou, O. (2013). Fuzzy assessment of health information system users' security awareness. *Journal of Medical Systems*, *37*(6), 1-13. https://doi.org/10.1007/s10916-013-9984-x

Björck, F. (2005, May). *Discovering information security management*. Stockholm University & Royal Institute of Technology. https://people.dsv.su.se/~bjorck/files/thesis-book.pdf

Bouhnik, D., & Deshen, M. (2014). Unethical behavior of youth in the Internet environment. *International Journal of Technology, Knowledge & Society: Annual Review*, *9*(2), 109-124. https://doi.org/10.18848/1832-3669/CGP/v09i02/56372

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548. https://doi.org/10.2307/25750690

Carmi, G., & Bouhnik, D. (2016). Functional analysis of applications for data security and for surfing privacy protection in the Internet. *International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC)*, *4*(7), 201-208. https://www.academia.edu/download/55017525/Functional_Analysis_of_Applications_for_Data_Security_and_for_Surfing_Privacy.pdf

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems*, *14*, 65-75. https://doi.org/10.17705/1CAIS.01403

Chen, H., & Li, W. (2019). Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective. *Behaviour & Information Technology*, *38*(5), 454-468. https://doi.org/10.1080/0144929X.2018.1539520

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98. https://doi.org/10.1287/isre.1070.0160

Eckersley, P. (2010). How unique is your web browser? In M. J. Atallah, & N. J. Hopper (Eds.), *Proceedings of the 10th International Symposium on Privacy Enhancing Technologies Symposium (PETS' 2010)*, *6205* (pp. 1-18). Berlin, Heidelberg: Springer-Verlag. https://doi.org/10.1007/978-3-642-14527-8_1

Fagerström, A. (2013). *Creating, maintaining and managing information security culture* [Master's Thesis. Arcada University of Applied Sciences]. https://www.theseus.fi/bitstream/handle/10024/63254/Fagerstrom_Alex.pdf

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley. https://people.umass.edu/aizen/f&a1975.html

Goh, S. C. (2003). Improving organizational learning capability: Lessons from two case studies. *The Learning Organization*, *10*(4), 216-227. https://doi.org/10.1108/09696470310476981

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69-79. https://doi.org/10.23919/SAIEE.2013.8531867

Harris, M. A., Furnell, S., & Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy and Security*, *10*(4) 186-202. https://doi.org/10.1080/15536548.2014.974429

Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Im, G. P., & Baskerville R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *36*(4), 68-79. https://doi.org/10.1145/1104004.1104010

Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R. A., Mashal, F. A., & Daas, F. (2014). Developing an ISO27001 information security management system for an educational institute: Hashemite University as a case study. *Jordan Journal of Mechanical and Industrial Engineering*, *8*(2), 102-118. http://jjmie.hu.edu.jo/vol%208-2/JJMIE-2014-8-2.pdf#page=60

Kotzias, P., Bilge, L., & Caballero, J. (2016). Measuring PUP prevalence and PUP distribution through pay-per-install services. In *Proceedings of the 25th USENIX Security Symposium (USENIX Security '16)* (pp. 739-756). Austin, TX: USENIX. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kotzias.pdf

Mcilwraith, A. (2006). *Information security and employee behaviour: How to reduce risk through employee education, training and awareness*. Routledge.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS '07)* (pp. 156-166). Waikoloa, HI: IEEE Press. https://doi.org/10.1109/HICSS.2007.206

Puhakainen, P. (2006). *A design theory for information security awareness* [Academic Dissertation]. Faculty of Science, University of Oulu. Oulu, Finland: Oulu University Press. http://jultika.oulu.fi/files/isbn9514281144.pdf

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757-778. https://doi.org/10.2307/25750704

Schlienger, T., & Teufel, S. (2002). Information security culture – The socio-cultural dimension in information security management. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Eds.), *Security in the information society: Visions and perspectives* (pp 191-201). Springer. https://doi.org/10.1007/978-0-387-35586-3_15

Scott, J. (2000). Rational choice theory. In G. Browning, A. Halcli, & F. Webster (Eds.), *Understanding contemporary society: Theories of the present* (pp. 126-138). SAGE Publications. https://doi.org/10.4135/9781446218310.n9

Stahl, B. C., Shaw, M., & Doherty, N. (2008). Information systems security management: A critical research agenda. In *Proceedings of SIGSEC Workshop on Information Security and Privacy (WISP 2008)* (pp. 5: 1-22). Paris, France: Association of Information Systems. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.566.1550&rep=rep1&type=pdf

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness in the home and work environments. In *Proceedings of the 5th International Conference on Availability, Reliability, and Security (ARES)* (pp. 196-203). Krakow, Poland: IEEE Press. https://doi.org/10.1109/ARES.2010.27

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333-365). Springer, Dordrecht. https://doi.org/10.1007/978-94-017-9385-8_14

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, *48*(6), 1143-1158. https://doi.org/10.5465/amj.2005.19573114

Wang, L., Cheng, M. Y. & Wang, S. (2018). Carrot or stick? The role of in-group/out-group on the multilevel relationship between authoritarian and differential leadership and employee turnover intention. *Journal of Business Ethics*, *152*(4), 1069-1084. https://doi.org/10.1007/s10551-016-3299-z

Weinberger, M., & Bouhnik, D. (2019). The strive for preserving online anonymity as a trigger for online identity falsification. *Systemics, Cybernetics and Informatics*, *17*(2), 22-24. http://www.iiisci.org/journal/CV$/sci/pdfs/HB068AU19.pdf

Weinberger, M., Zhitomirsky-Geffet, M., & Bouhnik, D. (2017). Factors affecting users' online privacy literacy among students in Israel. *Online Information Review*, *41*(5), 655-671. https://doi.org/10.1108/OIR-05-2016-0127

BIOGRAPHIES

Dr. Golan Carmi is a head of Information Technologies field at the Faculty of Management in the Jerusalem College of Technology. Investigate various aspects of virtual environments and information security, and published research in these areas. His professional interests include virtual environments, ICT technologies, mobile and internet security, knowledge management and digital innovation.

Prof. Dan Bouhnik is the head of the Computer Science Department at the Faculty of Engineering in the Jerusalem College of Technology. His research focuses on the connection between the worlds of computer technology, information and education. He is the author of a number of books used for teaching advanced computer science. His latest research deals with information security and privacy.