Strategic Rssearch on Social Problems in Iran University of Isfahan
Vol. 7, Issue 4, No. 23, Winter 2019
pp. 7-10
Received: 07.12.2017 Accepted: 05.07.2019

The Relationship between Information Security Awareness and the Intention to Violate Information Security with the Mediating Role of Individual Norms and Self-control

Hamid Reza Peikari*
Assistant Professor, Department of Public Administration, Islamic Azad University of Isfahan (Khorasgan), Isfahan, Iran
Babak Banazdeh
MA. Student, Department of Public Administration, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran
**Corresponding author, e-mail: h.peikari@khuisf.ac.ir*

Introduction
while the role of information in today's world cannot be denied, and since most activities and processes depend on information, the violation of information security is a critical concern. There are numerous motivations to threaten the security of an organization's information, ranging from economic motivations to revenge, although some threats are not intentional and the source of such threats does not really intend to do so. There are two sources of security threats, internal and external. The internal threats consist of the employees who intentionally or unintentionally violate the security rules of organizational information. While there are a variety of studies, dealing with this issue from different angles, researchers found no prior reports on the relationship between information security awareness and intention to violate information security with the mediating role of individual norms and self-control. Hence, this research aims to employ several theories, including general deterrence theory, general crime theory, control theory and social learning theory and suggests 5 minor hypotheses and 2 major hypotheses to examine the mentioned relationship among the employees of Keshavarzi Bank in Isfahan city. The results will lead to the development of a new theoretical model, which expands our knowledge in this field and also can be employed by researchers as the theoretical underpinning in their future research. The results can also offer new practical suggestions and solutions to reduce the incidents of information security breach in organizations by the employees.

Material & Methods

The present study is an applied research in terms of the purpose, and it is a descriptive-survey with correlation approach in terms of the method. The population of the present study consisted of 350 employees of Keshavarzi Bank in Isfahan. The studied sample was estimated 184 individuals based on the Morgan table and was selected by stratified random sampling fitted to size. The scale was adopted and adapted from published sources, and, except the demographics, was formatted on the five-point Likert scale. The demographics consisted of 5 questions, referring to the respondents' age, gender, education level, marital status, and organizational position. The main scale for the variable 'information security awareness' consisted of 3 dimensions, namely, 'information security general awareness', 'information security rules awareness', and 'information security violation sanctions', each consisted of three-question items. The questionnaires for 'individual norms' and 'intention to violate information security' each consisted of 4 items, and the questionnaire for 'self-control' consisted of 3 items. The validity of the questionnaires was obtained using face validity (by a number of respondents), content validity (by faculty members and management specialists) and construct validity (confirmatory factor analysis), using average variance extraction (AVE), composite reliability (CR), factor loading and Fornel and Larcker criterion. To examine the scale reliability, Cronbach's alpha was used and the overall reliability was 0.83. The collected data were analyzed by SPSS and SmartPLS software at two levels of descriptive and inferential statistics. Based on the results, all the research hypotheses were approved.

Discussion of Results & Conclusions

The relationships between awareness of information security with individual norms (β=0.67), self-control (β=0.71), and intention to violate information security (β=- 0.53) were significant. The results also indicated that individual norms (β= -0.54) and self-control (β= 0.48) were significantly related to intention to violate information security. The results are consistent with some past similar studies, which have been discussed. Overall, it can be suggested that employees' awareness regarding the security rules of the organization, and the consequences of violation of information security should be improved by conducting different classes.

Doi: 10.22108/ssoss.2019.108446.1174

Moreover, building an efficient security culture to encourage employees to follow the security rules of the organization can be an effective step toward this goal. Another step would be implementing sanctions in public against those who violate the security rules of the organization.

Keywords: Information Security Awareness, Intention to Violate Information Security, Individual Norms, Self-control.

References:

Abbaszadeh, M., Alizadeh Aghdam, M.B. & Parizad Benam, Sh. (2017) "Studying the Effect of Emotional Intelligence on Intentional High risky Behaviors of Drivers and its Dimensions." *Strategic Research on Social Problems in Iran*, 6: 1-16 (in Persian).

Ahmadi Jozi, M. (2016) "*A Study on the Organizational Culture and its Impact on the Information Security Management."* MA. Thesis, Khoramdare non-profit University (in Persian).

Amini, M. (2012) "*A Study on the Information Security Management Compliance in Isfahan Educational Hospitals*." MA. Thesis, Khomeini Shahr Islamic Azad University (in Persian).

Andreoni, J., Harbaugh, W. & Vesterlund, L. (2003) "The Carrot or the Stick: Rewards, Punishments, and Cooperation." *The American Economic Review*, 93: 893-902.

Anthony, V., Mikko, S. & Seppo, P. (2012) "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory." *Information & Management*, 49: 190-201

Boostani, D. (2011) "Social Capital and Risky Behaviour, Case: High School Students in Kerman, Mashhad." *Journal of Social Sciences*, 9: 1-31 (in Persian).

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010) "Information Security Policy Compliance: an Empirical Study of Rationality-based Beliefs and Information Security Awareness." *Management Information Systems*, 34: 523-548.

Chang. E. (2007) "An Investigation of Organizational Culture on Information Security Management." *Academy of Management Journal*, 35: 421-438

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 Researh*, 20 (1): 79–98.

D'Arcy, J., & Herath, T. (2011) "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings." *European Journal of Information Systems*, 20 (6): 643–58.

Esfandyarpour, A. (2010) "*The Factors Influencing the Acceptance of Information Security Policies among the Employees in Organizations."* MA. Thesis, Allameh Tabatabaei University (in Persian).

Fehr, E. & Schmidt, K. M. (2007) "Adding a Stick to the Carrot? The Interaction of Bonuses and Fines." *The American Economic Review*, 97: 177-181.

Ifinedo, P. (2014) "Information Systems Security Policy Compliance: an Empirical Study of the Effects of Socialization, Influence, and Cognition." *Information Management*, 51 (1): 69–79

Hasanzadeh, M., Karimzadegan, D., Moghaddam Jahangiri, N. (2011) "Presenting a Conceptual Frame for the Evaluation of Awareness Training on Information Security." *Information Services and Systems*, 1: 1-16 (in Persian).

Heidari Sareban, V. (2017) "Explanation Capital Social Relationship and Sense of Social Security in the Rural Areas, Case Study, Meshkinshar County." *Strategic Research on Social Problems in Iran*, 5: 45-62 (in Persian).

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011) "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?." *Communication of the ACM*, 54 (6): 59.

Karimi, Z. & Peikari, H.R. (2018) "The Impact of Nurses' Perception on the Information Security Training and Information Security Awareness on the Certainty and Severity of Information Security Violence Sanctions (Case: Specialized Training Hospitals in Isfahan)." *Nursing Training*, 7: 31-40 (in Persian).

Kathleen, M. E. (1985) "Control: Organizational and Economic Approaches." *Management Science* (pre-1986), 31: 134-142.

Khajouei, H. (2011) *"Information Security Controls."* MA. Thesis, Sistan Balouchestan University (in Persian).

Krishnan, R. (2003) "Information Security Management Systems." *Information Systems Research*, 1 (3): 255–76.

Li, H., Zhang, J., & Sarathy, R. (2010) "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory." *Decision Support Systems*, 48 (4): 635–645.

McCombs, B.L. (2008) "Self-regulated Learning and Academic Achievement: a Phenomenological View." In: Zimmerman BJ, Schunk DH, editors. *Self-regulated learning and academic achievement: theoretical perspectives*. Routledge; 63–118.

Mikko, S., Mahmood, M. A. & Seppo, P. (2014) "Employees' Adherence to Information Security

Policies: An Exploratory Field Study." *Information & Management*, 51: 217-224.

Mirchandani, D., & Motwani, J. (2003) "Reducing Internet Abuse in the Workplace." *SAM Advanced Management Journal*, 68 (1): 22–26.

Moody, G. D., & Siponen, M. (2013) "Using the Theory of Interpersonal Behavior to Explain Non-Work-Related Personal Use of the Internet at work". *Information & Management*, 50: 322–335.

Nakhaei, A. & Kheiry, B. (2012) "Investigating the Impact of Selected Factors on Consumer Green Purchase Intention." *Marketing Management*, 15: 105-130 (in Persian).

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009) "Studying Users' Computer Security Behavior: A Health Belief Perspective." *Decision Support Systems*, 46 (4): 815-825.

O'Donoghue, T., & Rabin, M. (2001) "*Healthcare Information Research, Chapter in Now or Later: Economic and Psychological Perspectives on Inter-temporal Choice*", edited by Roy Baumeister, George Loewenstein, and Daniel Read, published by Russell Sage Foundation Press.

Park, E., Kim, J., & Park, Y. S. (2017) "The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information." *Computers & Security*, 65: 64–76

Peikari, H.R., Ramayah T. Shah, M.H. & Lo, M.C. (2018) "Patients' Perception of the Information Security Management in Health Centers: The Role of Organizational and Human Factors." *BMC Medical Informatics and Decision Making*, 18: 102-107.

Purnaghdi, B. (2018) "Opportunities and Security Threats in Virtual Networks for Students." *Strategic Research on Social Problems in Iran*, 7: 25-35 (in Persian).

Sajadi, S.A. (2005) "Self-Control in Islamic Monitoring and Control (Considering Self-control on Islamic Theories)." *Honest Thought*, 23: 3-16 (in Persian).

Siegel, L.J. (2001). *Criminology: Theories, Patterns, and Typologies*. (7th ed). University of Massachusetts.

Song, Y., Lee, M., Jun, Y., Lee, Y., Cho, J. & Kwon, M., (2016) "Revision of the Measurement Tool for Patients' Health Information Protection Awareness." *Healthcare Informatics Research*, 22 (3): 206–216.

Skinner, W.F. & Fream, A. (1997) "A Social Learning Theory analysis of Computers Crime among College Students." *Journal of Research Crime Delinquency*, 34 (4): 495-518

Siponen, M., Pahnila, S. & Mahmood, M. A. (2010) "Compliance with Information Security Policies: An Empirical Investigation." *Computer*, 43 (2): 64 -71.

Straub, D.W. & Welke, R.J. (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making." *MIS Quarterly*, 22 (4): 441-69.

Straub, D.W. (1990) "Effective is Security: an Empirical Study." *Information Systems Research* 1 (3): 255-76.

Subramaniam, C., Park, S., & Kumar, R. L. (2008) "Understanding the Value of Countermeasure Portfolios in Information Systems Security." *Journal of Management Information Systems*, 25 (2): 241-280.

Thomas H., & Anderson, N. (2006) "Changes in New Comers' Psychological Contracts during Organizational Socialization: A Study of Recruits Entering the British Army." *Journal of Organizational Behavior*, 19: 745–67.

Vali, H. (2011) "*Identifying and Ranking the Influencing Factors on the Acceptance and Development of Information Security Policies in Organization."* MA. Thesis, Sistan Balouchestan University (in Persian).

Veiga. A., Martins, N. (2017) "Defining and Identifying Dominant Information Security Cultures and Subcultures." *Computers & Security*, 70: 72-94

Von Solms, R. (2014) "Information Security Management: Why Information Security is so Important." Information Management and Computer Security, 6 (4): 174 –77.

Wenzel, M. (2004) "The Social Side of Sanctions: Personal and Social Norms as Moderators of Deterrence." *Law and Human Behavior*, 28 (5): 547–567.

پژوهش‌های راهبردی مسائل اجتماعی ایران
سال هفتم، شماره پیاپی ۲۳، شماره چهارم، زمستان ۱۳۹۷
تاریخ دریافت: ۱۳۹۶/۰۹/۱۶ تاریخ پذیرش: ۱۳۹۸/۰۴/۱۵
صص ۴۱-۵۸

رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی عنوان مکرر: قصد نقض امنیت اطلاعات

حمیدرضا پیکری*، *استادیار، گروه مدیریت، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران*
بابک بنازاده، *دانشجوی کارشناسی‌ارشد مدیریت دولتی، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران*

چکیده
هدف پژوهش حاضر، بررسی رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی بین کارمندان بانک کشاورزی شهر اصفهان است. این پژوهش ازنظر هدف، کاربردی و ازنظر چگونگی اجرا توصیفی - همبستگی است. جامعهٔ آماری آن شامل ۳۵۰ نفر از کارکنان شعب بانک کشاورزی شهر اصفهان است که نمونهٔ بررسی‌شده براساس جدول مورگان و فرمول حجم نمونهٔ جامعهٔ محدود، ۱۸۴ نفر برآورد و به روش نمونه‌گیری در دسترس متناسب با حجم انتخاب شد. ابزار جمع‌آوری اطلاعات، پرسش‌نامهٔ بومی‌سازی شده بود. این پرسش‌نامه‌ها در طیف پنج‌درجه‌ای لیکرت تنظیم شده‌اند. روایی پرسش‌نامه‌ها با استفاده از روایی صوری (تعدادی از پاسخ‌دهندگان)، روایی محتوا (استاد راهنما و متخصصان رشتهٔ مدیریت) و روایی سازه (تحلیل عاملی) و پایایی آن ازطریق شاخص آلفای کرونباخ معادل ۰/۸۳ به دست آمد. اطلاعات جمع‌آوری شده با نرم‌افزار SPSS و PLS Smart ازطریق آزمون‌های آماری در دو سطح توصیفی و استنباطی تجزیه و تحلیل شد. آگاهی از امنیت اطلاعات با هنجارهای فردی (β=۰/۶۷)، خودکنترلی (β=۰/۷۱) و قصد نقض امنیت اطلاعات (β=-۰/۵۳) رابطهٔ معنادار دارد. همچنین نتایج نشان دادند هنجارهای فردی (β=-۰/۵۴) و خودکنترلی (β=-۰/۴۸) با قصد نقض امنیت اطلاعات رابطهٔ معنادار دارند.

واژه‌های کلیدی: آگاهی از امنیت اطلاعات، قصد نقض امنیت اطلاعات، هنجارهای فردی و خودکنترلی

* نویسندهٔ مسئول: ۰۹۱۷۳۱۴۶۵۱۴
Email: h.peikari@khuisf.ac.ir

Doi: 10.22108/ssoss.2019.108446.1174

مقدمه و بیان مسئله

جهان امروز از جوامع اطلاعات‌محور تشکیل شده است که اصلی‌ترین ویژگی آن اهمیت و استفاده از اطلاعات و ارتباطات در امور جاری است (Krishnan, 2003). نقش بی‌بدیل اطلاعات در تصمیم‌گیری‌ها و همچنین پیشرفت سریع فناوری اطلاعات موجب تبدیل جوامع امروزی به جوامع اطلاعاتی شده است. امروزه نقش پراهمیت اطلاعات در جوامع و حساسیت فرایندهای جمع‌آوری، ثبت و انتشار اطلاعات، دگرگونی بنیادینی را در ساختار مناسبات و ارتباطات جوامع ایجاد کرده و همین امر، موجب ایجاد مخاطرات، تهدیدها و نگرانی‌های جدیدی مبتنی بر اطلاعات شده است که مقولهٔ رفتارهای پرخطر دربارهٔ اطلاعات از آن جمله است (پورنقدی، ۱۳۹۷). رفتارهای پرخطر، رفتارهای بالقوهٔ مخربی‌اند که افراد یک جامعه، به‌طور ارادی یا حتی بدون اطلاع از پیامدها و عواقب نامطلوب احتمالی، آنها را انجام می‌دهند (بوستانی، ۱۳۹۱: ۲) که از آن جمله، نقض امنیت اطلاعات است (پورنقدی، ۱۳۹۷). این رفتارهای ضداجتماعی مهم‌ترین چالش‌های بهداشتی و روانی – اجتماعی در یک جامعه‌اند (عباس‌زاده و همکاران، ۱۳۹۶: ۲). بررسی اسناد و مدارک نشان می‌دهد امنیت مترادف مفهوم «سلامتی» به کار رفته و وجود آن ضامن سلامتی جامعه پنداشته شده است (حیدری‌ساربان، ۱۳۹۶: ۴۶)؛ بنابراین، این امر، برنامه‌ریزی دقیق برای شناسایی عوامل مؤثر در مدیریت و کنترل آن را برای ارتقای سلامت روانی جامعه می‌طلبد. اهمیت این مسئله به این دلیل است که امروزه نیازها، کسب و کار، تجارت، امور مالی و بانکی ازطریق تبادل اطلاعات برطرف می‌شوند؛ بنابراین، اهمیت امنیت اطلاعات دوچندان می‌شود (Krishnan, 2003). به همین دلیل، در صورت نقض امنیت اطلاعات، سازمان‌ها و افراد دچار تشویش خاطر و احساس ناامنی می‌شوند؛ درنتیجه، به‌دلیل نقش حفاظت از امنیت اطلاعات حساس افراد در سلامت و بهداشت روانی جامعه، شناسایی عواملی که در نقض امنیت اطلاعات نقش دارند و موجبات به خطر افتادن سلامت روانی جامعه را فراهم می‌کنند، اهمیت بسزایی دارد. در همین راستا، یکی از مهم‌ترین عناصر در مدیریت امنیت اطلاعات، کارمندان سازمان‌ها هستند (کریمی و پیکری، ۱۳۹۷).

مانند دیگر سطوح جامعه، سازمان‌های امروزی به جمع‌آوری، ثبت و انتشار اطلاعات نیاز دارند؛ بنابراین، درک آنچه موجب می‌شود کارمندان، اقدامات امنیتی مربوط به اطلاعات را بپذیرند یا در مقابل آن مقاومت کنند، حیاتی است (اسفندیارپور، ۱۳۸۹). امروزه بسیاری از بانک‌ها دریافته‌اند که برای موفقیت، علاوه بر استفاده از روش‌ها و فناوری‌های امنیتی، به سرمایه‌گذاری و برنامه‌ریزی برای ایجاد یک برنامهٔ جامع امنیت نیازمندند تا بدان طریق از افشای اطلاعات حساس خود که از یک سو موجب خسارت‌دیدن فعالیت‌های بانکداری و ازسوی دیگر، موجب نگرانی مشتریان خود و از دست دادن اعتماد آنها می‌شود، جلوگیری کنند. برنامهٔ جامع امنیت بانکداری الکترونیک شامل فناوری‌ها و برنامه‌های حفاظتی – فناوری‌های موجود (نرم‌افزار و سخت‌افزار)، افراد و برنامه‌های مدیریتی مرتبط با حفاظت از منابع و عملیات بانکداری – است. با وجود این، موفقیت چنین برنامه‌هایی به مدیریت نیروی انسانی سازمان و برنامه‌ریزی برای تغییر رفتار امنیتی آنها بستگی دارد (کریمی و پیکری، ۱۳۹۷). به عبارت دیگر، علاوه بر اهمیت استفاده از فناوری‌های به‌روز و پیشرفته برای حفاظت از امنیت اطلاعات، نگرش و رفتار کارمندان نیز در حفاظت از امنیت اطلاعات سازمان نقش اساس دارد (D'arcy & Herath, 2011). پژوهشگران در مطالعه‌ای گزارش کردند که بیشتر دلایل نقض امنیت اطلاعات به فاکتورهای مرتبط به افراد برمی‌گردد (کریمی و پیکری، ۱۳۹۷)؛ به‌طوری که حتی راه حل فنی بالاتر از حد نیاز را برای سازمان مضر دانستند. طبق یافته‌های آنها، در صورت ایجاد همهٔ تمهیدات فنی و سیاست‌های امنیتی، آگاهی‌نداشتن و بی‌توجهی کارمندان می‌تواند همهٔ حفاظت‌های فنی را بی‌نتیجه کند؛ در صورتی که کارمندان آگاه در محیط کاری تا اندازهٔ زیادی موجب کاهش

این خطرات امنیتی می‌شوند (Kruger & Kearney, 2006)؛ بنابراین، ارتقای چگونگی رفتار کارکنان بستر مناسبی برای ارتقای اثربخشی امنیت اطلاعات در درون بانک فراهم می‌کند و مدیریت بانک باید با تدوین برنامه‌ها و سیاست‌های مناسب و اثرگذار در این حوزه، سعی در مدیریت امنیت اطلاعات در بانک داشته باشد.

در این زمینه و براساس نظریهٔ بازدارندگی عمومی، یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقای آگاهی کاربران از امنیت اطلاعات است (D'arcy & Herath, 2011; D'arcy et al., 2009). در این صورت، افراد آگاهی‌های لازم و مربوط به نقش و مسؤلیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می‌کنند. بنابراین آموزش کارکنان و افزایش آگاهی آنها دربارهٔ امنیت اطلاعات، می‌توانند تأثیر جالب‌توجهی در حفاظت از اطلاعات سازمان داشته باشند (ولی، ۱۳۹۱؛ کریمی و پیکری، ۱۳۹۷).

رابطهٔ بین آگاهی از امنیت اطلاعات در سازمان با ارزش‌های شخصی (خودکنترلی و هنجارهای شخصی) و قصد نقض اطلاعات را می‌توان با استناد به نظریهٔ یادگیری اجتماعی، نظریهٔ عمومی جرم و نظریهٔ کنترل توضیح داد (Skinner & Fream, 1997; Park et al., 2017). براساس نظر اودونگو و رابین (2001)، آگاهی بر رفتار خودکنترلی افراد تأثیر دارد. در خودکنترلی، عامل کنترل‌کننده از محیط به انسان منتقل می‌شود؛ به‌طوری که شخص با اختیار و آگاهی عملکرد خود را در قالب استانداردهای مشخص و درجهت اهداف مطلوب ارزیابی و اصلاح می‌کند (سجادی، ۱۳۸۵). پژوهش‌های انجام‌شده نشان می‌دهند هنجارهای شخصی به‌صورت مستقیم بر رفتارهای انحرافی تأثیر می‌گذارند (Song et al., 2016). کارمندانی که آگاهی از امنیت اطلاعات در سطح بالا دارند، ممکن است هنجارهای فردی سطح بالا هم داشته باشند که این هنجارها با به‌کارگیری روش‌های آموزشی در بانک‌ها شکل گرفته‌اند. در مطالعات گذشته گزارش شده است که آگاهی با هنجار فردی رابطه دارد. چنانکه ایفندو[1] (2014) گزارش کرده است، در صورتی که آگاهی دانش‌آموزان در زمینهٔ رفتارهای ضداجتماعی افزایش یابد، این امر بر ارزش‌ها و هنجارهای آنها تأثیر خواهد داشت. از آنجا که طبق نظریهٔ عمل منطقی، ارزش‌های فردی در تعیین رفتار فرد مؤثر است، می‌توان نتیجه گرفت دربارهٔ سیاست‌های امنیتی اگر فردی خودکنترلی بالایی داشته باشد، تمایل کمتری به افشای اطلاعات دارد (سجادی، ۱۳۸۵)؛ بنابراین، کارکنانی که هنجارهای شخصی بالایی دارند، خود را با سیاست‌های استفاده از اینترنت بیشتر تطبیق می‌دهند و نگرش آنها با سیاست‌های امنیتی سازگاری دارد و تمایل کمتری به افشای اطلاعات سازمان دارند (Park et al., 2017)؛ بنابراین، انتظار می‌رود هنجارهای فردی و خودکنترلی در ارتباط بین آگاهی افراد در زمینهٔ امنیت اطلاعات و رفتار آنها دربارهٔ امنیت اطلاعات نقش میانجی داشته باشد.

در همین راستا، هدف این پژوهش تعیین رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی است. انجام این مطالعه، علاوه بر ارائه و آزمودن یک الگوی نظری جدید در حوزهٔ امنیت اطلاعات از منظر انسانی – که می‌تواند به پژوهشگران و جامعهٔ علمی در زمینهٔ درک بهتر چگونگی مدیریت و حفاظت از امنیت اطلاعات از منظر نیروی انسانی سازمان کمک کند – می‌تواند مبنای نظری جدیدی را برای مطالعات بعدی و گسترش الگوی ارائه‌شده به‌وسیلهٔ پژوهشگران دیگر فراهم کند. یافته‌ها همچنین می‌توانند شامل پیشنهادها و راهکارهای کاربردی جدیدی برای سیاست‌گذاری در حوزهٔ مدیریت امنیت اطلاعات باشند.

مرور ادبیات پژوهش

قصد نقض امنیت اطلاعات: امنیت اطلاعات به معنای حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز

[1] Ifinedo

است. این فعالیت‌ها عبارت‌اند از: دسترسی، استفاده، افشا، خواندن، نسخه‌برداری یا ضبط، خراب‌کردن، تغییر و دستکاری (سادوسکای و همکاران، ۱۳۸۴). قصد نقض امنیت اطلاعات یعنی رعایت‌نکردن محدودیت‌ها و قوانین مرتبط با امنیت اطلاعات و نقض اطلاعات که ممکن است تبعاتی برای کسب و کار داشته باشد و جبران آن ماه‌ها و سال‌ها طول بکشد که ناآگاهی یا اطلاع ناقص از مقررات و قوانین یا اشتباهات، فرصت‌های زیادی برای افشای اطلاعات سازمان در اختیار رقبا قرار می‌دهد (ولی، ۱۳۹۱).

آگاهی از امنیت اطلاعات: آگاهی‌های لازم و مربوط به نقش و مسئولیت افراد در حفظ امنیت اطلاعات در کار مربوط به خود را گویند. آگاهی از امنیت اطلاعات در افراد سبب تغییر رفتار آنها و تقویت فعالیت‌های خوب امنیتی می‌شود و به افراد اجازه می‌دهد نسبت به امنیت فناوری اطلاعات نگران و پاسخگو باشند (حسن‌زاده و همکاران، ۱۳۹۱). آگاهی از امنیت اطلاعات طبق نظر پارک و همکاران شامل سه بعد زیر است: الف) آگاهی عمومی از امنیت اطلاعات به معنای آگاهی‌رسانی عمومی در زمینهٔ ابعاد امنیت، ازجمله اهداف یک سیستم مدیریت امنیت اطلاعات است که با هدف افزایش آگاهی عمومی کاربران و جامعهٔ مخاطبان سیستم‌های مدیریت امنیت اطلاعات، صورت می‌گیرد (Park et al., 2017). ب) آگاهی از قوانین امنیت اطلاعات که یک مفهوم ساختاری جدید است که به آگاهی، درک و رعایت کارکنان از سیاست‌ها، قوانین و اطلاعات امنیتی سازمان مرتبط اشاره و بیان می‌کند که آگاهی کارکنان از سیاست امنیت اطلاعات سازمان تأثیر مثبتی بر نگرش کارکنان برای موافقت با سیاست‌های امنیتی شرکت دارد (Bulgurcu et al., 2010). ج) آگاهی از شدت مجازات نقض امنیت اطلاعات به دانش و درک درست کارکنان از انواع مجازات و شدت مجازات‌های مرتبط با نقض امنیت اطلاعات سازمان اطلاق می‌شود (Park et al., 2017). بلگورسو و همکاران[1] (2010) نشان دادند آگاهی عمومی از اطلاعات امنیتی زیرمجموعهٔ آگاهی امنیت اطلاعات است که تأثیر مثبتی در نگرش به‌سوی موافقت با سیاست امنیتی اطلاعاتی سازمان دارد. کارمندان بانک به درک مفهوم کلی از امنیت اطلاعات و مسائل برای محافظت مناسب از اطلاعات سلامتی بیماران نیاز دارند.

خودکنترلی: هرگاه عامل کنترل‌کننده از خارج به داخل انسان منتقل شود، به‌طوری که شخص با اختیار و آگاهی، عملکرد خود را در قالب استانداردهای مشخص و در جهت اهداف مطلوب ارزیابی و اصلاح کند، خودکنترلی تحقق یافته است (سجادی، ۱۳۸۵). نظریهٔ کنترل به دیدگاهی بازمی‌گردد که دربارهٔ کنترل انسان بحث می‌کند. نظریه‌های کنترل اجتماعی، بزهکاری را به متغیرهای عادی جامعه نسبت می‌دهند. نظریه‌پردازان کنترل اجتماعی در این باور مشترک‌اند که آنچه باید تشریح شود این است که چرا مردم از قانون پیروی می‌کنند. جزء مهم تمام نظریه‌های کنترل اجتماعی، تلاش برای تشریح عوامل بازدارندهٔ مردم از ارتکاب جرم است (ویلیامز و مک‌شین، ۱۳۹۱). نظریهٔ عمومی جرم از دیگر نظریه‌هایی است که در این زمینه از آن بهره برده شده است. این نظریه، مفاهیم نظریهٔ کنترل را با دیدگاه‌های زیست اجتماعی، روان‌شناختی، فعالیت روزمره و نظریه‌های انتخاب عقلانی ترکیب می‌کند (Siegel, 2001). نظریهٔ عمومی جرم، مدعی است افراد با هدف کسب لذت و احتراز از رنج، مرتکب جرم می‌شوند؛ بنابراین، جرم امری منطقی، عقلانی و پیش‌بینی‌پذیر است. افراد زمانی مرتکب جرم می‌شوند که این امر پاداش‌دهنده و عامل خودکنترلی غایب باشد. خودکنترلی، ایجاد حالتی درون فرد است که او را به انجام وظایفش متمایل می‌کند، بدون آنکه عامل خارجی بر او کنترل داشته باشد.

هنجاری‌های فردی: هنجارهایی‌اند که اثر بازدارندگی قوی بر رفتارهای انحرافی افراد دارند و دانش کافی دربارهٔ اخلاق، اینکه چه چیزی درست و چه چیزی نادرست است و

[1] Bulgurcu et al.

اینکه کدامین رفتار مناسب است، ارائه می‌دهند (Li et al., 2010: 638). در اصطلاح جامعه‌شناسی هنجارها را الگوهای استانداردشدهٔ رفتار می‌گویند. این الگوها نشان‌دهندهٔ رفتار ایده‌آل یا مطلوب جامعه‌اند. هنجارها در جامعه‌شناسی به‌منزلهٔ یک قاعدهٔ رفتاری عمل می‌کنند که هم افراد برای انجام کارها از آن پیروی می‌کنند و هم رفتار انسان‌ها با آن سنجیده می‌شود؛ بنابراین، هنجارهای اجتماعی‌اند که تعیین می‌کنند انسان چه باید بگوید و از گفتن چه چیزهایی باید اجتناب ورزد. باید چگونه بیندیشد و چگونه رفتار کند (بیرو، ۱۳۷۵). هنجارها از این بابت بر ارزش‌ها و نگرش‌های اجتماعی اثر می‌گذارند که تجویزکننده و در عین حال نهی‌کنندهٔ رفتارها هستند. هنجارهای اجتماعی را تجلی بیرونی ارزش‌های اجتماعی می‌دانند. هنجارها به این دلیل باقی می‌مانند که با نظام ارزشی جامعه توافق دارند و به نیازهای اجتماعی پاسخ می‌دهند (سلیمی و داوری، ۱۳۸۰). پژوهش‌های پیشین به این نتیجه رسیده‌اند که هنجارهای ذهنی نسبت به نگرش‌ها، در پیش‌بینی مقاصد رفتاری افراد نقش مهم‌تری دارند (نخعی و خیری، ۱۳۹۱).

مروری بر پژوهش‌های پیشین

کریمی و پیکری (۱۳۹۷) در پژوهشی توصیفی – میدانی با نام «تأثیر ادراک پرستاران از آموزش امنیت اطلاعات و آگاهی از سیاست‌های امنیت اطلاعات بر ادراک از شدت و قطعیت مجازات نقض امنیت اطلاعات»، تأثیر ادراک کارکنان از قطعیت و شدت مجازات‌های افشای اطلاعات را بر قصد آنها برای سوءاستفاده از اطلاعات بررسی کردند. نمونهٔ بررسی‌شده در این پژوهش ۱۲۴ نفر از کارکنان بیمارستان چمران شهر اصفهان بود. فرضیه‌ها با نرم‌افزار Smart PLS تجزیه و تحلیل شدند. نتایج پژوهش نشان دادند ادراک کارکنان از شدت و قطعیت مجازات‌ها تأثیر منفی بر افشای اطلاعات دارد. آگاهی کارکنان از سیاست‌های امنیتی سیستم‌های اطلاعاتی تأثیر مثبت معنادار بر ادراک آنها نسبت به شدت و قطعیت مجازات افشای اطلاعات و آگاهی‌شان از برنامه‌های آموزشی آگاهی و امنیتی، تأثیر مثبت معنادار بر ادراک آنها نسبت به شدت و قطعیت مجازات افشای اطلاعات دارد. همچنین آگاهی کارکنان از شیوه‌های نظارت بر کامپیوتر، تأثیر مثبت معنادار بر ادراک آنها نسبت به شدت و قطعیت مجازات افشای اطلاعات دارد.

احمدی‌جزئی (۱۳۹۵) در پژوهش «بررسی فرهنگ سازمانی و تأثیر آن بر مدیریت امنیت اطلاعات» با توجه به سطح آمادگی کارکنان قوهٔ قضاییه به این نتیجه دست یافت که فرهنگ سازمانی مشارکتی بر محرمانه‌بودن و دردسترس بودن اطلاعات اثرگذار بوده است؛ ولی بر پیوستگی اطلاعات و پاسخگویی اثرگذار نبوده است. همچنین فرهنگ ثبات بر هر چهار مؤلفهٔ امنیت اطلاعات اثرگذار بوده است؛ ولی فرهنگ نوآوری و فرهنگ اثربخشی بر هیچ‌کدام از مؤلفه‌های امنیت اطلاعات تأثیرگذار نبوده است.

خواجویی (۱۳۹۰) در پژوهش «بررسی کنترل‌های امنیت اطلاعات»، حوزه‌های مدیریتی و اهداف کنترلی امنیت اطلاعات را براساس استاندارد مدیریت امنیت اطلاعات اولویت‌بندی کرد. او برای بررسی استاندارد مدیریت امنیت اطلاعات از روش تحلیل سلسله‌مراتبی فازی و برای گردآوری داده‌های پژوهش از پرسش‌نامه‌ای مشتمل بر ۱۴۴ مقایسهٔ زوجی استفاده کرد. جامعهٔ این پژوهش مناطق چهارگانهٔ شرکت ملی پخش فرآورده‌های نفتی ایران در منطقهٔ شرق و جنوب‌شرق کشور شامل کرمان، زاهدان، خراسان جنوبی و چابهار بود که به‌دلیل محدودبودن تعداد اعضای کمیته‌های راهبری این چهار منطقه، از روش سرشماری در نمونه‌گیری استفاده شد. بعد از تجزیه و تحلیل داده‌ها ضریب ناسازگاری ۰/۰۵ برای پرسش‌نامه‌های پژوهش به دست آمد که این مقدار کمتر از ۰/۱ و مقداری پذیرفتنی بود. نتایج حاصل از پژوهش نشان می‌دهند حوزه‌های مدیریتی کنترل دسترسی و اکتساب، بهبود، حفظ و نگهداری سیستم‌های اطلاعاتی به ترتیب با اوزان محلی ۰/۱۲۴ و ۰/۱۲۱ اولویت‌های اول و دوم و مدیریت دارایی با وزن محلی ۰/۰۳۶ اولویت آخر را میان ۱۱ حوزهٔ پژوهش به خود

اختصاص دادند. همچنین میان اهداف کنترلی، مدیریت دسترسی کاربر و مدیریت تحویل خدمت شخص سوم به ترتیب با اوزان جهانی ۰/۰۴۷ و ۰/۰۰۷ اولویت‌های اول و آخر را میان ۳۹ هدف کنترلی امنیت به خود اختصاص دادند.

اسفندیارپور (۱۳۸۹) در پژوهش پیمایشیِ «عوامل مؤثر بر پذیرش سیاست‌های امنیت اطلاعات توسط کارمندان در سازمان»، عوامل مؤثر بر پذیرش سیاست‌های امنیت اطلاعات در سازمان را با نظرخواهی از ۸۵ نفر در سازمان وزارت کشور بررسی کرد. نتایج پژوهش نشان دادند تعهد سازمانی و تأثیرات اجتماعی، تأثیر فزاینده‌ای در پذیرش سیاست‌های امنیت اطلاعات دارند و در دسترس بودن منابع فاکتوری اثرگذار در ارتقای خودباوری و عاملی پیش‌بینی‌کننده در پذیرش سیاست‌های امنیت اطلاعات خواهد بود. اگرچه سازمان‌ها از فناوری‌ها و فعالیت‌های امنیتی استفاده می‌کنند، این اثبات شده است که امنیت اطلاعات تنها با ابزارهای فناورانه به دست نمی‌آید؛ درنتیجه، سازمان‌ها به سیاست‌های امنیت اطلاعات توجه می‌کنند. بیشتر سازمان‌ها زمان و منابع برای تهیه، ایجاد و نگهداری سیاست‌های امنیت صرف می‌کنند؛ در حالی که اگر کاربران سیستم‌های اطلاعاتی سازمان تمایلی برای پیروی از سیاست‌ها نداشته باشند این کوشش‌ها شکست خواهند خورد. همچنین نتایج نشان دادند: ۱) تأثیرات اجتماعی تأثیر فزاینده‌ای بر نیت قبول (قصد پذیرش سیاست امنیت اطلاعات) دارند؛ ۲) در دسترس بودن منابع تأثیر فزاینده‌ای بر ارتقای خودباوری و به همان اندازه نیات قبول سیاست دارد؛ ۳) تعهد سازمانی نقشی مضاعف ازطریق تأثیر مستقیم بر نیات و به همان اندازه طرز تفکر دربارهٔ سیاست دارد.

پارک و همکاران[1] (2017) نقش آموزش امنیت اطلاعات و عوامل فردی در افشای اطلاعات سلامت (پزشکی) بیماران را بر گسترش امنیت اطلاعات بررسی کردند. با توجه به بیشترشدن اهمیت اجابت مقررات و سیاست‌های امنیت اطلاعات به‌وسیلهٔ کارکنانی که در صنعت مراقبت‌های بهداشتی کار می‌کنند، بحث امنیت اطلاعات در مراکز درمانی از اهمیت بیشتری برخوردار شده است. همچنین یافته‌های این پژوهش نشان دادند امنیت اطلاعات و ارزش‌های شخصی در آموزش پرستاری و تلاش صنعت مراقبت‌های بهداشتی برای حفاظت از اطلاعات سلامت بیماران نقش جالب‌توجهی دارند.

وایگا و مارتینز[2] (2017) در پژوهش «بهبود فرهنگ امنیتی اطلاعات ازطریق اقدامات نظارت و پیاده‌سازی» که بین ۵۱۲ نفر از کارکنان در آفریقای جنوبی انجام دادند، به این نتیجه دست یافتند که ابزار ارزیابی فرهنگ امنیت اطلاعات می‌تواند در سازمان‌ها به‌طور موفقیت‌آمیزی بر فرهنگ امنیت اطلاعات تأثیر بگذارد. همچنین آموزش امنیت اطلاعات و آگاهی، عاملی مهم در تأثیرگذاری مثبت بر فرهنگ امنیتی اطلاعات هنگام استفاده از ارزیابی فرهنگ امنیت اطلاعات است. آنها نشان دادند فرهنگ و خرده‌فرهنگ‌های امنیتی اطلاعات غالب در طول زمان پس از اجرای مداخلات هدفمند به یک فرهنگ امنیتی اطلاعاتی مثبت‌تر بهبود یافته است.

بلگورسو و همکاران (2010) در پژوهش «انطباق سیاست امنیتی اطلاعات: اعتقادات مبتنی بر عقلانیت و آگاهی از امنیت اطلاعات»، انواع مجازات و شدت مجازات‌های مرتبط با نقض امنیت اطلاعات سلامت را بررسی کردند. نتایج پژوهش آنها نشان دادند رابطه‌ای مثبت و معنادار بین شدت تنبیه و قصد موافقت با سیاست امنیت اطلاعات در سازمان وجود دارد. همچنین نتایج پژوهش آنها نشان دادند تأثیر نقض امنیت اطلاعات محافظت‌شده، می‌تواند بسیار جدی‌تر از نقض سیاست امنیتی در یک سازمان باشد؛ ازاین‌رو، به اعمال مجازات‌های شدیدتر نیاز است.

دارسی و همکاران[3] (2009) در پژوهش «آگاهی کاربر از اقدامات مخالف امنیت و تأثیر آن در سیستم‌های اطلاعاتی با رویکرد بازدارنده»، تأثیر آگاهی کاربر از اقدامات مخالف

[1] Park et al.

[2] Veiga & Martins

[3] D'Arcy et al.

امنیت بر سیستم‌های اطلاعاتی را بررسی کردند. نتایج پژوهش آنها نشان دادند برنامه‌های آموزشی امنیت می‌توانند هم سطح درک افراد از تحریم‌ها و هم شدت درک‌شده از تحریم را افزایش دهند. همچنین شدت تحریم دریافت‌شده تأثیر منفی بر هدف سوءاستفاده دارد.

چانگ[1] (2007) در پژوهش «بررسی فرهنگ سازمانی بر مدیریت امنیت اطلاعات» که بین پرستاران انجام شد، به این نتیجه دست یافت که فرهنگ سازمانی، تأثیر مستقیم بر ایجاد فرهنگ امنیت اطلاعات دارد. او مؤلفه‌های سازمانی ازجمله همکاری، نوآوری، سازگاری، کارآیی و تأثیربخشی بر اصول امنیت اطلاعات (محرمانه‌بودن، در دسترس بودن، صحت و پاسخگویی) را بررسی کرد. یافته‌ها نشان دادند تمام عوامل فرهنگ سازمانی بر مؤلفه‌های امنیت اطلاعات تأثیر مثبتی دارند.

توماس و اندرسون[2] (2006) در پژوهش «پرورش یک فرهنگ امنیتی اطلاعات سازمانی» که بین ۸۱۰ نفر از کارکنان یک شرکت بین‌المللی در اروپا انجام دادند، به این نتیجه دست یافتند که یک راه حل امنیتی باید جزئی اساسی در هر سازمان باشد. یکی از مهم‌ترین مشکلات در دست‌یابی به جذب اطلاعات به یک سازمان، اعمال و رفتار کارکنان است. برای اطمینان از ادغام امنیت اطلاعات به فرهنگ سازمانی یک سازمان، حفاظت از اطلاعات باید بخشی از فعالیت‌های روزمره و رفتار دوم شخصیت کارکنان باشد.

مطالعات پیشین عوامل متعددی را در زمینهٔ عوامل انسانی نقض یا حفاظت از امنیت اطلاعات بررسی کرده‌اند؛ اما هیچ کدام از آنها، رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی را مطالعه نکرده‌اند.

چارچوب نظری پژوهش

نظریهٔ بازدارندگی عمومی به‌طور گسترده‌ای برای مطالعهٔ انطباق رفتار کارکنان در سازمان استفاده می‌شود. این نظریه به استفاده از راهبرد فشار منفی (مجازات) برای پرهیز از رفتارهای غیرایمن و ناخواسته با افزایش شدت و قطعیت مجازت اشاره دارد (Straub & Welke, 1998; Straub, 1990). برخی پژوهشگران استدلال می‌کنند که پاداش (تشویقی و انگیزه) اگر به‌منزلهٔ راهبرد اجرایی مثبت به کار گرفته شود، ممکن است به دست‌یابی رفتار انطباقی بهتر کمک کند. به‌طور مشابه اگر پاداش با تحریم همراه باشد، بر ارزیابی هزینه – فایدهٔ کارکنان از رفتار انطباقی و رفتار غیرانطباقی تأثیر می‌گذارد (Bulgurcu et al., 2010). اجرای مؤثر سازوکار کنترل به چگونگی اجرا و شیوهٔ به‌کارگیری آن بستگی دارد. به هر حال تا به امروز مطالعه‌ای برای تحلیل تعامل مؤثر بین مجازات و پاداش دربارهٔ موضوع پیروی و سیاست‌های امنیتی انجام نشده است. با مرور مقالات و پژوهش‌ها، تضادهایی در ادبیات مربوط به تطابق امنیت یافت می‌شود. تأثیر پاداش در پیروی از سیاست‌های امنیتی در سازمان‌ها به نظر متناقض است: سیاست پاداش در تأثیرگذاری بر قصد کارکنان به پیروی جواب نمی‌دهد (Mikko et al., 2014)؛ این در حالی است که برخی مطالعات نشان می‌دهند پاداش، ابزاری مثبت در جهت مشارکت کارکنان در پیروی از امنیت است (Bulgurcu et al., 2010). اگرچه استفاده از مجازات و پاداش موضوعی بسیار جالب در حوزه‌هایی مانند جامعه‌شناسی، روان‌شناسی اجتماعی و رفتار سازمانی است، هیچ مدرکی در مستندات مربوط به پیروی از سیاست‌های امنیتی سیستم‌های اطلاعاتی و حفظ اطلاعات حساس مشتریان وجود ندارد که تأیید کند این مسئله به‌طور واقعی عمل خواهد کرد (Fehr & Schmidt, 2007; Andreoni et al., 2003).

نظریهٔ بازدارندگی فرض می‌کند افراد دراساس انتخاب عقلانی و منطقی دارند و انتخاب آنها برای ارتکاب جرم به منفعتی بستگی دارد که آن جرم یا جنایت ممکن است برای آنها داشته باشد و افراد کمتر مستعد به مشارکت در یک رفتار مجرمانه‌اند؛ از این جهت که قطعیت، شدت و سرعت

[1] Chang
[2] Thomas & Anderson

مجازاتی که علیه آن جرم تعیین شده است، از منافع آن بیشتر است (Hu et al., 2011; Siponen et al., 2010). نظریهٔ بازدارندگی عمومی که در خط‌مشی سیستم‌های اطلاعاتی و حفظ حریم شخصی مشتریان به کار رفته است، بیان می‌کند که با استفاده از فن‌های بازدارندگی عمومی مانند منع‌کردن، پیشگیری، تشخیص و ارائهٔ راه حل، امکان کاهش تهدیدها و کاهش یا حذف ریسک وجود دارد (Subramaniam et al., 2008).

آگاهی از امنیت اطلاعات و ارزش‌های فردی

چنانکه پیش از این بیان شد، نظریهٔ یادگیری اجتماعی، نظریهٔ عمومی جرم و نظریهٔ کنترل رابطهٔ بین دو متغیر آگاهی از امنیت اطلاعات در سازمان با ارزش‌های شخصی (خودکنترلی و هنجارهای شخصی) و قصد نقض اطلاعات را ازحیث نظری توجیه می‌کنند (Skinner & Fream, 1997; Park et al., 2017).

پژوهش‌های انجام‌شده نشان می‌دهند هنجارهای شخصی بر رفتارهای انحرافی به‌صورتی مستقیم تأثیر می‌گذارند (Song et al., 2016). در مطالعات پیشین گزارش شده است که آگاهی با هنجار فردی رابطه دارد؛ چنانکه ایفندو (2014) گزارش داد در صورتی که آگاهی دانش‌آموزان در زمینهٔ رفتارهای ضداجتماعی افزایش یابد، این امر بر ارزش‌ها و هنجارهای آنها تأثیر خواهد داشت. کارمندانی که آگاهی از امنیت اطلاعات سطح بالا دارند، ممکن است هنجارهای فردی سطح بالا هم داشته باشند که این هنجارها ازطریق به‌کارگیری روش‌های آموزشی در بانک‌ها شکل گرفته‌اند. آموزش عاملی حیاتی و تأثیرگذار در شکل‌گیری هنجارهای فردی کارمندان است. کارمندان می‌توانند ارزش‌ها و دیدگاه‌های خود را دربارهٔ محرمانه نگه‌داشتن اطلاعات بانکی – مالی افراد ازطریق گذراندن برنامه‌های تنظیم‌شده دربارهٔ اطلاع و آگاهی‌ها از امنیت اطلاعات در درهٔ آموزشی شکل دهند؛ بنابراین، فرضیه‌های فرعی این پژوهش به شکل زیر خواهند بود:

فرضیهٔ ۱– آگاهی از امنیت اطلاعات با هنجارهای فردی رابطهٔ معناداری دارد.

نظریهٔ بازدارندگی تمرکزی ویژه بر خودکنترلی در رفتارهای انحرافی دارد. فرض اساسی مطالعات پیشین بر این است که افرادی که خودکنترلی پایینی دارند، رفتارهای ضداجتماعی از خود نشان می‌دهند؛ بنابراین، یکی از اهداف آموزش باید کمک به افراد در توسعهٔ خودکنترلی‌شان باشد (Park et al., 2017). براساس نظر اودونگو و رابین[1] (2001)، آگاهی بر رفتار خودکنترلی افراد تأثیر دارد؛ درواقع، افرادی که ازطریق برنامه‌های مختلف آگاهی از امنیت اطلاعات پزشکی به سطوح بالایی از آگاهی از امنیت اطلاعات دست یافته‌اند، خودکنترلی بالاتری دارند (Park et al., 2017)؛ ازاین‌رو، در فرضیهٔ فرعی دوم چنین ادعا می‌شود:

فرضیهٔ ۲– آگاهی از امنیت اطلاعات با خودکنترلی رابطهٔ معناداری دارد.

آگاهی از محرمانه‌بودن و قصد نقض امنیت اطلاعات بانکی – مالی

در مطالعات مربوط به امنیت اطلاعات رفتاری، نظریهٔ بازدارندگی عمومی اهمیت بسزایی دارد. در این زمینه و براساس نظریهٔ بازدارندگی عمومی، یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقای آگاهی کاربران از امنیت اطلاعات است (D'arcy & Herath, 2011; D'arcy et al., 2009). بولگورسو و همکاران (2010) در بررسی‌های خود به این نتیجه رسیدند که هم آگاهی از امنیت اطلاعات عمومی و هم آگاهی از ضوابط و سیاست‌های امنیت اطلاعاتی، تأثیری مثبت بر نگرش موافق با سیاست امنیتی اطلاعاتی دارند. در این صورت، افراد آگاهی‌های لازم و مربوط به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می‌کنند. آگاهی از امنیت اطلاعات در افراد سبب تغییر رفتار و تقویت فعالیت‌های خوب امنیتی

[1] O'Donoghue & Rabin

می‌شود و به افراد اجازه می‌دهد نسبت به امنیت فناوری اطلاعات نگران و پاسخگو باشند (Von Solms, 2014). برنامه‌های آموزش امنیت و آگاهی می‌توانند رفتارهای انحرافی مرتبط با امنیت اطلاعات بانکی را ازطریق آموزش کارکنان دربارهٔ اهمیت امنیت اطلاعات عمومی، مجازات رفتارهای انحرافی و برخوردهای متقابل در سازمان‌ها کاهش دهند. دارسی و همکاران (2009) بدین نتیجه رسیده‌اند که برنامه‌های آموزش امنیت و آگاهی قادرند هم سطح درک افراد از مجازات و هم شدت درک‌شده از مجازات را افزایش دهند. در زمینهٔ اطلاعات بانکی و مالی، ذی‌نفعان ازجمله کارمندان بانک – که به درجات بالایی از آگاهی از امنیت اطلاعات ازطریق روش‌هایی که در بانک آموزش دیده‌اند، دست‌یافته‌اند – تمایل کمتری به رفتارهای انحرافی به‌ویژه افشای اطلاعاتی مشتریان دارند؛ بنابراین، در فرضیهٔ فرعی سوم ادعا می‌شود که:

فرضیه ۳- آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات رابطهٔ معناداری دارد.

ارزش‌های فردی و تمایل به نقض امنیت اطلاعات بانکی – مالی

در مطالعهٔ حاضر آگاهی از امنیت اطلاعات به‌منزلهٔ دانش عمومی یک کارمند در زمینهٔ امنیت اطلاعات و دانش دربارهٔ قوانین و مقررات امنیتی و موانع مربوط به آن تعریف شده است. در همین راستا، مطالعات قبلی نشان می‌دهند برنامه‌های آموزش و امنیت و آگاهی اثرات جالب‌توجه بازدارندهٔ مهمی در کنترل رفتارهای انحرافی دارند (کریمی و پیکری، ۱۳۹۷). همچنین بلگورسو و همکاران (2010) دریافتند که آگاهی عمومی از امنیت اطلاعات و آگاهی از سیاست امنیتی اطلاعات تأثیر مثبت بر نگرش کارکنان برای موافقت با سیاست‌های امنیتی شرکت دارند. همچنین، طبق نظریهٔ عمل منطقی، ارزش‌ها و هنجارهای افراد با چگونگی رفتار آنها مرتبط است. افرادی که سطوح بالایی از هنجارهای شخصی (برای مثال، اخلاق) را دارند، دانش کافی دربارهٔ اخلاق، اینکه چه چیزی درست و چه چیزی نادرست است و اینکه کدامین رفتار مناسب است، دارند. ادبیات جرم‌شناسی چنین بیان می‌کند که هنجارهای شخصی اثر بازدارندگی قوی بر رفتارهای انحرافی افراد دارند. لی و همکاران[1] (2010) بدین نتیجه رسیده‌اند که هنجارهای فردی به‌طور معمول در زمینهٔ این است که فرد از خود رفتارهای انحرافی نشان دهد یا ملاحظات اخلاقی خود را وارد رفتارهای خویش کند؛ درواقع، هنجارهای شخصی به‌صورتی مستقیم بر رفتارهای انحرافی تأثیر می‌گذارند. در مطالعهٔ حاضر، اگر باورهای فردی بر این باشند که افشای اطلاعات بانکی افراد ازلحاظ اخلاقی نادرست است، فرد تمایل کمتری به افشای چنین اطلاعاتی خواهد داشت.

بنابراین، در فرضیهٔ فرعی چهارم چنین ادعا می‌شود:

فرضیهٔ ۴- هنجارهای فردی با قصد نقض امنیت اطلاعات رابطهٔ معناداری دارند.

پژوهش‌های جرم‌شناسی همراه با فراتحلیل‌ها، اهمیت تأثیر خودکنترلی را بر رفتارهای انحرافی نشان داده‌اند. براساس نظریهٔ یادگیری اجتماعی، نظریهٔ عمومی جرم و نظریهٔ کنترل، انتظار می‌رود آگاهی از امنیت اطلاعات در سازمان، بر ارزش‌های شخصی مانند خودکنترلی و قصد نقض اطلاعات تأثیر بگذارد (Skinner & Fream, 1997; Park et al., 2017). افرادی که خودکنترلی پایینی دارند، تمایل بیشتری برای رفتن به‌دنبال ریسک و خطر، فعالیت‌های فیزیکی زیاد، ارتباطات غیرکلامی، کوته‌فکری و خلق‌وخوی تند دارند (McCombs, 2008). افرادی که ضمن داشتن چنین ویژگی‌هایی، خودکنترلی پایینی هم دارند، رفتارهای انحرافی مانند نقض امنیت اطلاعات را بیشتر از خود نشان می‌دهند. در این مقاله، چنین فرض شده است که اگر فردی خودکنترلی بالایی داشته باشد، تمایل کمتری به افشای اطلاعات پزشکی دارد؛ بنابراین، در فرضیهٔ فرعی پنجم ادعا می‌شود که:

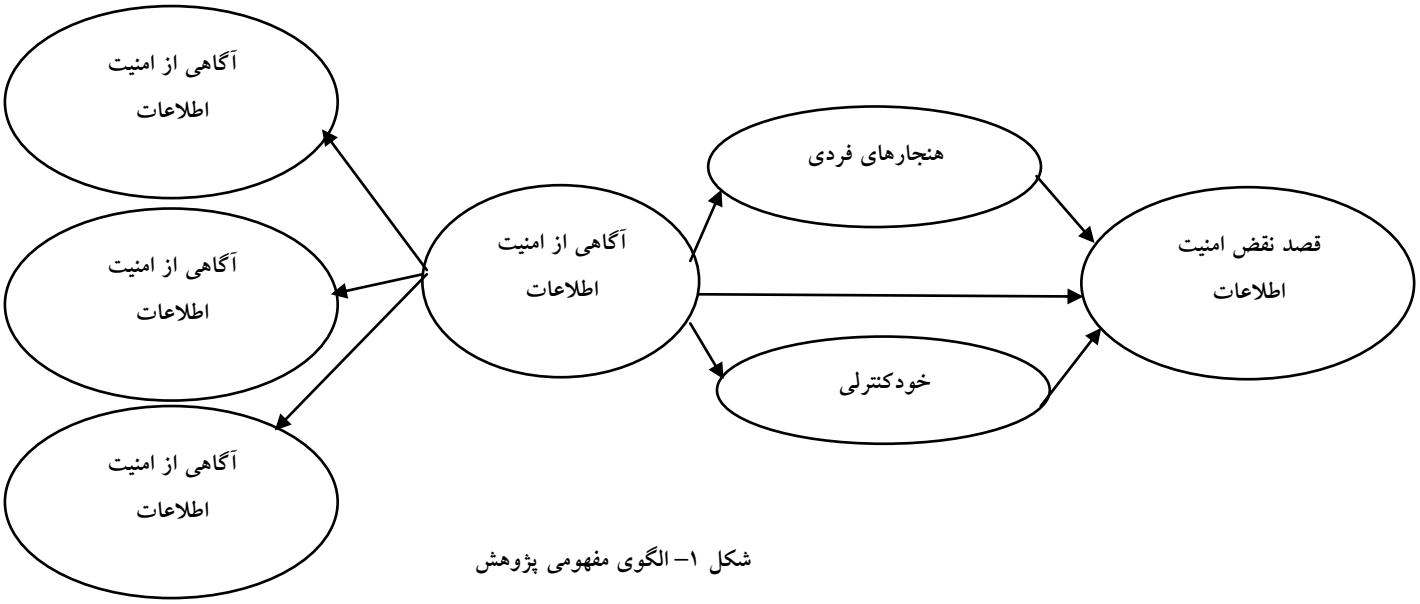
[1] Li et al.

فرضیهٔ ۵- خودکنترلی رابطهٔ منفی با تمایل کارکنان به افشای اطلاعات بانکی مشتریان دارد.

با توجه به ۵ فرضیهٔ فرعی ذکرشده، ۲ فرضیه اصلی زیر پیشنهاد می‌شود:

فرضیهٔ اصلی اول: آگاهی از امنیت اطلاعات با نقش میانجی کامل هنجارهای فردی با قصد نقض امنیت اطلاعات رابطه دارد.

فرضیهٔ اصلی دوم: آگاهی از امنیت اطلاعات با نقش میانجی کامل خودکنترلی با قصد نقض امنیت اطلاعات رابطه دارد.



شکل ۱- الگوی مفهومی پژوهش

روش پژوهش

پژوهش حاضر از نوع کاربردی و یک مطالعهٔ توصیفی - همبستگی است. جامعهٔ آن، ۳۵۰ نفر از کارکنان شعب بانک کشاورزی شهر اصفهان بود. دلیل انتخاب بانک به‌منزلهٔ جامعهٔ مطالعه‌شده این بود که چون موضوع این پژوهش دربارهٔ عوامل مؤثر بر نقض امنیت اطلاعات بود، به‌طور طبیعی جامعهٔ مطالعه‌شده باید به اطلاعات حساسی دسترسی داشته باشند تا حفاظت یا نقض آن موضوعیت یابد و مطالعهٔ آن اهمیت داشته باشد. به عبارت دیگر، انجام این پژوهش با توجه به پدیدهٔ مطالعه‌شده دربارهٔ همهٔ اعضای جامعه موضوعیت نداشت. ازطرفی، از آنجا که موضوع امنیت اطلاعات در بانک‌ها اهمیت بسزایی دارد، انجام این پژوهش در بانک‌ها را توجیه می‌کرد. دلیل انتخاب یک بانک به‌منزلهٔ جامعهٔ مطالعه‌شده نیز این بود که پژوهشگران سعی داشتند با مطالعهٔ موضوع بین کارمندان یک سازمان، نقش و دامنهٔ تغییر عواملی مانند فرهنگ سازمانی، هنجارهای گروهی و عوامل مدیریتی را ثابت یا حداقل نگه دارند؛ در حالی که در صورت مطالعهٔ چند بانک به‌طور همزمان، این عوامل ممکن بود از عوامل مؤثر در پیش‌بینی احتمال نقض امنیت اطلاعات محسوب شوند. بر همین اساس، نمونهٔ پژوهش با استفاده از جدول مورگان ۱۸۴ نفر بود که با استفاده از روش نمونه‌گیری غیرتصادفی تعیین شدند و پس از توزیع ۲۱۵ پرسش‌نامه، تعداد ۱۹۷ پرسش‌نامهٔ کاربردی جمع‌آوری شد.

جدول ۱– مشخصات ابزار، پایایی و روایی

متغیر		منبع سؤالات	آلفای کرونباخ	متوسط واریانس استخراج‌شده (AVE)	پایایی مرکب (CR)
آگاهی از امنیت اطلاعات	آگاهی عمومی از امنیت اطلاعات	بلگورسو و همکاران (2010)	۰/۹۱	۰/۷۸	۰/۹۲
	آگاهی از قوانین امنیت اطلاعات	بلگورسو و همکاران (2010)	۰/۸۳	۰/۷۵	۰/۹۰
	آگاهی از شدت مجازات نقض امنیت اطلاعات	ایفندو (2014)	۰/۷۵	۰/۸۷	۰/۸۶
	قصد نقض امنیت اطلاعات	پرینسلی و همکاران (2016)	۰/۷۴	۰/۸۵	۰/۸۵
	هنجارهای فردی	لی و همکاران (2010)	۰/۸۱	۰/۷۳	۰/۸۹
	خودکنترلی	دارسی و همکاران (2009)	۰/۸۱	۰/۷۴	۰/۸۷

چنانکه در جدول ۱ نشان داده شده است، پرسش‌نامهٔ استفاده‌شده برای سنجش متغیرها از مقالات چاپ‌شده در مجلات معتبر بین‌المللی اقتباس و بومی‌سازی و در طیف لیکرت طراحی شده است. روایی صوری و محتوایی پرسش‌نامه با توجه به نظرهای تعدادی از افراد جامعهٔ آماری و استادان و صاحب‌نظران سنجیده شد. روایی سازه با استفاده از تحلیل عاملی تأییدی و پایایی پرسش‌نامه با استفاده از آلفای کرونباخ سنجیده شد. برای بررسی روایی سازه از سه شاخص پایایی مرکب، متوسط واریانس استخراج‌شده و بار عاملی استفاده شد. مقادیر پایایی مرکب همهٔ متغیرها از ۰/۷ و متوسط واریانس استخراج‌شده از ۰/۵ بیشتر شده است. به‌علاوه، بار عاملی تمام گویه‌ها از ۰/۵ بیشتر شده است. همچنین چنانکه در جدول ۲ ذکر شده است، قاعدهٔ فورنل–لارکر رعایت شده است؛ درنتیجه، روایی واگرا و همگرا تأیید شده است که این امر بیان‌کنندهٔ روایی پذیرفتنی سازه در این مطالعه است. همچنین چنانکه در جدول ۱ ذکر شده است، آلفای کرونباخ برای هر یک از متغیرها بیش از ۰/۷ است که بیان‌کنندهٔ پایایی ابزار استفاده‌شده است. این مطالعه برای تحلیل داده‌ها از روش تحلیل توصیفی با نرم‌افزار SPSS و روش حداقل مربعات جزئی با نرم‌افزار SmartPLS استفاده کرده است.

جدول ۲– قاعدهٔ فورنل – لارکر

	آگاهی عمومی	آگاهی از قوانین	آگاهی از شدت مجازات	قصد نقض امنیت اطلاعات	هنجارهای فردی	خودکنترلی
آگاهی عمومی‌از امنیت اطلاعات	۰/۸۸					
آگاهی از قوانین امنیت اطلاعات	۰/۵۵	۰/۸۶				
آگاهی از شدت مجازات نقض امنیت اطلاعات	۰/۵۹	۰/۶۹	۰/۹۳			
قصد نقض امنیت اطلاعات	۰/۶۰	۰/۵۳	۰/۶۴	۰/۹۲		
هنجارهای فردی	۰/۵۴	۰/۵۸	۰/۶۴	۰/۵۶	۰/۸۵	
خودکنترلی	۰/۶۸	۰/۶۳	۰/۶۰	۰/۴۹	۰/۴۹	۰/۸۶

یافته‌ها

یافته‌های جمعیت‌شناختی

جدول ۳- توصیف آماری ویژگی‌های جمعیت‌شناختی جامعه

	متغیرها	فراوانی	درصد
جنسیت	مذکر	۱۲۸	۰/۶۵
	مؤنث	۶۹	۰/۳۵
سن	کمتر از ۳۰ سال	۴۷	۲۳/۹
	۳۹-۳۱ سال	۱۰۰	۵۰/۸
	۴۹-۴۰ سال	۴۰	۲۰/۳
	بیش از ۵۰ سال	۱۰	۵/۱
تحصیلات	دیپلم	۱۶	۸/۱
	کاردانی	۴۵	۲۲/۸
	کارشناسی	۱۲۳	۶۲/۴
	کارشناسی‌ارشد و بیشتر	۱۳	۶/۶
وضعیت تأهل	مجرد	۴۲	۲۱/۳
	متأهل	۱۵۵	۷۸/۷
سمت	رییس	۷	۳/۶
	معاون شعبه	۲۲	۱۱/۲
	کارمند	۱۶۸	۸۵/۳

نتایج حاصل از آمار توصیفی در جدول ۳ نشان می‌دهند از مجموع ۱۹۷ نفر، بیشترین تعداد پاسخ‌دهندگان کارکنان مرد و کمترین تعداد پاسخ‌دهندگان زن بودند. افراد دارای سن ۳۱ تا ۳۹ سال بیشترین نفرات از جامعهٔ آماری پژوهش و افراد با سن ۵۰ سال کمترین نفرات از جامعهٔ آماری پژوهش را تشکیل دادند. کارکنان دارای سمت کارمند بیشترین تعداد و کارکنان دارای سمت رییس شعبه کمترین تعداد پاسخ‌دهندگان‌اند. افراد دارای تحصیلات کارشناسی بیشترین تعداد از جامعهٔ آماری را تشکیل داده‌اند و افرادی کمترین نمونه را تشکیل داده‌اند که تحصیلات کارشناسی‌ارشد و بالاتر دارند. افراد متأهل بیشترین تعداد و افراد مجرد کمترین تعداد از جامعهٔ آماری را تشکیل داده‌اند. میانگین آگاهی، خودکنترلی، هنجار فردی و قصد نقض امنیت اطلاعات در مقیاس ۵، ۲/۹۵، ۳/۱۸، ۳/۳۶، و ۲/۷۲ بود.

نتایج فرضیه‌ها

نتایج فرضیه‌های اصلی

فرضیهٔ اصلی اول: آگاهی از امنیت اطلاعات با نقش میانجی هنجارهای فردی با قصد نقض امنیت اطلاعات رابطه دارد.

آزمون سوبل برای انجام استنباط دربارهٔ ضریب اثر غیرمستقیم استفاده می‌شود. با داشتن برآوردی از خطای استاندارد مسیرها می‌توان p-value را محاسبه کرد.

در این رابطه:

a ضریب مسیر میان متغیر مستقل و میانجی (امنیت اطلاعات بر هنجارهای فردی) (۰/۶۷)؛

b ضریب مسیر میان متغیر میانجی و وابسته (هنجارهای فردی بر قصد نقض امنیت اطلاعات) (۰/۵۴-)؛

Sa خطای استاندارد مسیر متغیر مستقل و میانجی (۰/۰۶)؛

Sb خطای استاندارد مسیر متغیر میانجی و وابسته (۰/۰۱).

$$Z - Value = \frac{a * b}{\sqrt{(b^2 * s_a^2) + (a^2 * s_b^2) + (s_a^2 * s_b^2)}}$$

طبق فرمول ذکرشده مقدار آزمون ۱۰/۹- است و از آنجا که از ۱/۹۶- بیشتر است، اثر غیرمستقیم معنی‌دار دارد.

برای تعیین اثر غیرمستقیم از آمارهٔ VAF استفاده می‌شود که مقداری بین ۰ تا ۱ است و هرچه به عدد یک نزدیک‌تر باشد، نشان‌دهندهٔ اثر قوی متغیر میانجی است.

$$VAF = \frac{a*b}{(a*b)+c}$$

در این فرمول C ضریب مسیر میان متغیر مستقل و وابسته است.

$$VAF = 40$$

یعنی ۴۰ درصد رابطهٔ امنیت با نقض اطلاعات ازطریق اثر غیرمستقیم هنجار فردی صورت می‌گیرد.

فرضیهٔ اصلی دوم: آگاهی از امنیت اطلاعات با نقش میانجی خودکنترلی بر قصد نقض امنیت اطلاعات تأثیر دارد.

در این رابطه:

a ضریب مسیر میان متغیر مستقل و میانجی (امنیت اطلاعات بر خودکنترلی) (۰/۷۱)؛

b ضریب مسیر میان متغیر میانجی و وابسته (خودکنترلی بر قصد نقض امنیت) (۰/۴۸-)؛

Sa خطای استاندارد مسیر متغیر مستقل و میانجی (۰/۰۳)؛

Sb خطای استاندارد مسیر متغیر میانجی و وابسته (۰/۰۵).

$$Z - Value = \frac{a * b}{\sqrt{(b^2 * s_a^2) + (a^2 * s_b^2) + (s_a^2 * s_b^2)}}$$

Z-value = -8/8

طبق فرمول ذکرشده مقدار آزمون ۸/۸- است و از آنجا که از ۱/۹۶- بیشتر است، اثر غیرمستقیم معنی‌دار دارد.

برای تعیین اثر غیرمستقیم از آمارهٔ VAF استفاده شد.

$$VAF = \frac{a*b}{(a*b)+c}$$

در این فرمول C ضریب مسیر میان متغیر مستقل و وابسته است (آگاهی از امنیت اطلاعات بر نقض اطلاعات)

c=۰/۵۳

VAF=38

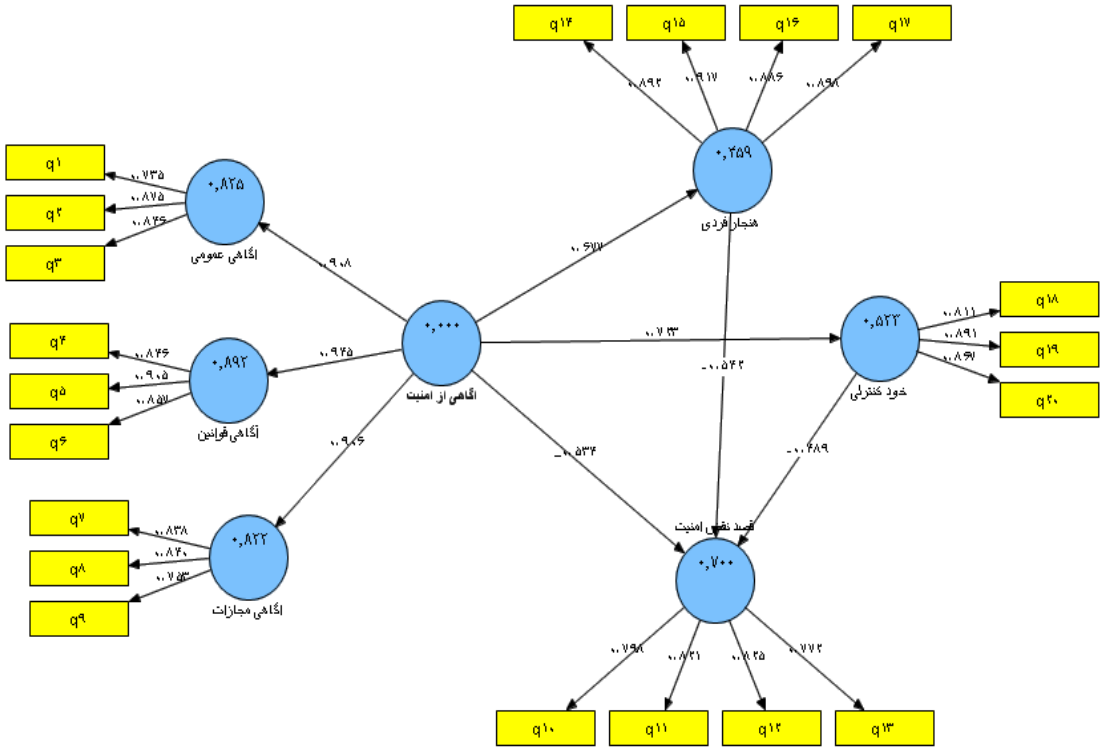
یعنی ۳۸ درصد رابطهٔ آگاهی از امنیت اطلاعات با نقض اطلاعات ازطریق اثر غیرمستقیم خودکنترلی صورت می‌گیرد.

نتایج فرضیه‌های فرعی

چنانکه در جدول ۴ نشان داده شده است، نتایج تحلیل معادلهٔ ساختاری نشان می‌دهند ضریب معناداری مسیر میان تمام متغیرها از ۱/۹۶ بیشتر است که معناداری مسیر و تأیید تمام فرضیه‌ها را نشان می‌دهد. با توجه به مقدار ضریب استانداردشده می‌توان گفت یک واحد تغییر متغیر آگاهی از امنیت اطلاعات ۰/۶۷ واحد تغییر در متغیر هنجارهای فردی، ۰/۷۱ واحد تغییر در خودکنترلی و ۰/۵۳- واحد تغییر در قصد نقض امنیت اطلاعات بین کارمندان بانک ایجاد می‌کند. نتایج تحلیل معادلهٔ ساختاری نشان می‌دهند یک واحد تغییر در هنجارهای فردی و خودکنترلی به ترتیب ۰/۵۴- و ۰/۴۸- واحد تغییر در قصد نقض امنیت اطلاعات بین کارمندان بانک ایجاد می‌کند.

جدول ۴- نتایج فرضیه‌های فرعی پژوهش

فرضیهٔ پژوهش	آمارهٔ t	ضریب استانداردشده	مقدار p	نتیجهٔ فرضیه
آگاهی از امنیت اطلاعات و هنجارهای فردی	۱۱/۲	۰/۶۷	۰/۰۱	تأیید فرضیه
آگاهی از امنیت اطلاعات و خودکنترلی	۱۳	۰/۷۲	۰/۰۱	تأیید فرضیه
آگاهی از امنیت اطلاعات و قصد نقض امنیت اطلاعات	۵/۳	۰/۵۳-	۰/۰۱	تأیید فرضیه
هنجارهای فردی و قصد نقض امنیت اطلاعات	۲/۳	۰/۵۴-	۰/۰۵	تأیید فرضیه
خودکنترلی و قصد نقض امنیت اطلاعات	۳/۲	۰/۴۸-	۰/۰۱	تأیید فرضیه



شکل ۲- ضرایب مسیر و بارهای عاملی

نتیجه

امروزه نقش پراهمیت اطلاعات در جوامع و حساسیت فرایندهای جمع‌آوری، ثبت و انتشار اطلاعات، دگرگونی بنیادینی را در ساختار مناسبات و ارتباطات جوامع ایجاد کرده است و همین امر، موجب ایجاد مخاطرات، تهدیدها و نگرانی‌های جدید مبتنی بر اطلاعات شده است که مقولهٔ رفتارهای پرخطر دربارهٔ اطلاعات از آن جمله است. این رفتارهای ضداجتماعی مهم‌ترین چالش‌های بهداشتی و روانی - اجتماعی است؛ درنتیجه، به‌دلیل نقش حفاظت از امنیت اطلاعات حساس افراد در سلامت و بهداشت روانی جامعه، شناسایی عواملی که در نقض امنیت اطلاعات نقش دارند و موجب به خطر افتادن سلامت روانی جامعه می‌شوند، اهمیت بسزایی دارد. یکی از مهم‌ترین عناصر در مدیریت امنیت اطلاعات، کارمندان سازمان‌ها هستند. هدف پژوهش حاضر، تعیین رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی در شعب بانک کشاورزی شهر اصفهان است.

در فرضیهٔ اصلی اول و دوم ادعا شد که آگاهی از امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی با قصد نقض امنیت اطلاعات رابطه دارد. نتایج تحلیل معادلهٔ ساختاری جدول ۴ نشان می‌دهند رابطهٔ مستقیم بین آگاهی از امنیت اطلاعات و قصد نقض امنیت اطلاعات ۰/۵۳- است و رابطهٔ غیرمستقیم ازطریق هنجارهای فردی ۴۰ درصد و ازطریق خودکنترلی ۳۸ درصد است. این به آن معناست که آگاهی از امنیت اطلاعات با نقش میانجی هنجارهای فردی تا ۴۰ درصد و با نقش میانجی خودکنترلی تا ۳۸ درصد با قصد نقض امنیت اطلاعات رابطه دارد و هر دو فرضیهٔ اصلی تأیید می‌شوند. در تبیین این یافته‌ها می‌توان گفت آگاهی افراد از امنیت اطلاعات (شامل آگاهی از مسائل دربارهٔ امنیت اطلاعات و عواقب نقض امنیت اطلاعات) موجب می‌شود

آنها از نقض امنیت اطلاعات اجتناب کنند. همچنین بهبود هنجارهای فردی را در پی خواهد داشت که این موضوع نیز سبب کاهش قصد نقض امنیت اطلاعات می‌شود. ازطرف دیگر، می‌توان گفت افرادی که آگاهی کافی از امنیت اطلاعات و عواقب نقض آن دارند، به‌دلیل آگاهی از عواقب آن به‌احتمال زیاد از نقض امنیت اطلاعات اجتناب می‌کنند. همچنین این آگاهی موجب افزایش خودکنترلی آنان خواهد شد که این امر به‌صورت غیرمستقیم سبب کاهش قصد نقض امنیت اطلاعات می‌شود. نتایج حاصل‌شده از پژوهش حاضر با نتایج مطالعات متعددی همسوست که در ادامه به آنها اشاره شده است:

در فرضیهٔ فرعی اول ادعا شد که آگاهی از امنیت اطلاعات با هنجارهای فردی رابطهٔ معناداری دارد. نتایج تحلیل معادلهٔ ساختاری نشان‌دهندهٔ معنی‌دار بودن این رابطه در سطح اطمینان ۹۹ درصد است که سبب تأیید این فرضیه می‌شود. نتایج حاصل‌شده از پژوهش حاضر مبنی بر رابطهٔ مثبت و معنادار آگاهی از امنیت اطلاعات با هنجارهای فردی، با نتایج پژوهش ایفندو (2014) و سونگ و همکاران[1] (2016) همسوست. در تبیین این فرض می‌توان گفت افرادی که سطح بالایی از آگاهی امنیت اطلاعات دارند، ممکن است هنجارهای فردی سطح بالا هم داشته باشند. افراد ارزش‌ها و دیدگاه‌های خود را دربارهٔ محرمانه نگه‌داشتن اطلاعات دیگران ازطریق گذراندن برنامه‌های تنظیم‌شده شکل می‌دهند؛ بنابراین، افرادی که از آموزش امنیت اطلاعات برخوردار بوده‌اند، هنجارهای شخصی بالاتری در این زمینه دارند و خود را با سیاست‌های امنیت اطلاعات بیشتر تطبیق می‌دهند و نگرش آنها با سیاست‌های امنیتی سازگاری بیشتری دارد.

در فرضیهٔ فرعی دوم ادعا شد که آگاهی از امنیت اطلاعات با خودکنترلی رابطهٔ معناداری دارد. نتایج تحلیل معادلهٔ ساختاری نشان‌دهندهٔ معنی‌دار بودن اثر در سطح اطمینان ۹۹ درصد است که سبب تأیید این فرضیه می‌شود. نتایج حاصل، با نتایج پژوهش پارک و همکاران (2017) و اودونگو و رابین (2001) همسوست. در تبیین این فرض می‌توان گفت آموزش آگاهی‌های امنیتی به‌منزلهٔ روشی برای توسعهٔ رفتار افراد در پیروی از سیاست‌های امنیتی کمک می‌کند که این مهم رابطهٔ زیادی با خودکنترلی افراد خواهد داشت. برنامه‌های آموزشی امنیت اطلاعات می‌توانند سبب بالارفتن درک افراد از نوع و شدت مجازات مربوط به نقض امنیت اطلاعات بشوند. افرادی که ازطریق آموزش به درک و تجربهٔ بالایی در زمینهٔ آگاهی از امنیت اطلاعات برسند، سعی در کنترل رفتار خود در رویارویی با شرایط و موقعیت‌های پرخطر خواهند داشت.

در فرضیهٔ فرعی سوم ادعا شد که آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات رابطهٔ معناداری دارد. نتایج تحلیل معادلهٔ ساختاری نشان می‌دهند این فرضیه در سطح اطمینان ۹۹ درصد معنادار و نوع رابطه معکوس است. نتایج حاصل‌شده از پژوهش حاضر مبنی بر رابطهٔ مثبت و معنادار آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نتایج پژوهش ون سولمز[2] (2014)، بلگورسو و همکاران (2010) و دارسی و همکاران (2009) هم‌راستاست. در تبیین این فرضیه می‌توان گفت برنامه‌های آگاهی از امنیت اطلاعات می‌توانند رفتارهای انحرافی مرتبط با امنیت اطلاعات را ازطریق آموزش افراد دربارهٔ اهمیت امنیت اطلاعات عمومی، مجازات رفتارهای انحرافی و برخوردهای متقابل کاهش دهند. برنامه‌های آموزشی امنیت اطلاعات می‌توانند سبب بالارفتن درک افراد از نوع و شدت مجازات‌ها شوند. افرادی که ازطریق آموزش به درک و تجربهٔ بالایی دربارهٔ آگاهی‌های امنیت اطلاعات برسند، تمایل کمتری به رفتارهای انحرافی و پرخطر به‌ویژه افشای اطلاعات حساس دارند. براساس نتایج پژوهش پیشنهاد می‌شود دوره‌های آموزشی به‌صورت غیرحضوری و از راه دور در زمینهٔ سیاست‌های امنیت اطلاعات و عواقب نقض آنها برگزار شود.

براساس یافته‌های فرضیه‌های اول، دوم و سوم پیشنهاد

[1] Song et al.

[2] Von Solms

می‌شود ایجاد تشکیلات موردنیاز برای ایجاد و تداوم امنیت فضای تبادل اطلاعات، اجرای طرح‌ها و برنامه‌های امنیتی و آگاهی‌دادن به افراد ازطریق دوره‌های آموزشی نسبت به تهدیدات بالقوه دربارهٔ امنیت اطلاعات، در جریان قراردادن افراد دربارهٔ خطرات مربوط به نقض امنیت اطلاعات، ارائهٔ دوره‌های آموزشی دربارهٔ رعایت دستورالعمل‌ها و مسئولیت‌پذیر بودن در قبال اجرای خط‌مشی‌ها، حفاظت از امنیت اطلاعات و تشویق و پاداش به افرادی که دربارهٔ حفاظت از اطلاعات حساس تلاش می‌کنند، در دستور کار قرار گیرد.

در فرضیهٔ فرعی چهارم ادعا شد هنجارهای فردی با قصد نقض امنیت‌اطلاعات رابطهٔ معناداری دارن. نتایج نشان‌دهندهٔ معنی‌دار بودن رابطه در سطح اطمینان ۹۵٪ بود که سبب تأیید این فرضیه می‌شود و نوع رابطه معکوس است. نتایج به‌دست‌آمده با نتایج پژوهش کریمی و پیکری (۱۳۹۷)، بلگورسو و همکاران (2010) و لی و همکاران (2010) همسوست. در تبیین این نتیجه می‌توان گفت هنجارهای شخصی اثر بازدارندگی قوی بر رفتارهای انحرافی افراد دارند؛ به آن دلیل که افراد ملاحظات اخلاقی و هنجارهای شخصی خود را در رفتارهای خود دخیل می‌کنند؛ بنابراین، باورهای فردی افرادی که هنجارهای شخصی بالایی دارند، بر این است که افشای اطلاعات دیگران ازلحاظ اخلاقی نادرست است و تمایل کمتری به افشای اطلاعاتی خواهند داشت. براساس نتایج پژوهش پیشنهاد می‌شود فرهنگ‌سازی ازطریق آموزش با موضوع پیروی از دستورالعمل‌ها دربارهٔ امنیت اطلاعات دیگران و همچنین برخورد با افرادی که دستورالعمل‌های سازمان دربارهٔ اطلاعات حساب شخصی مشتریان را افشا می‌کنند، در دستور کار قرار گیرد.

در فرضیهٔ فرعی پنجم ادعا شد که خودکنترلی با قصد نقض امنیت اطلاعات رابطهٔ معناداری دارد. نتایج تحلیل نشان می‌دهند این رابطه در سطح اطمینان ۹۹ درصد معنی‌دار و نوع رابطه معکوس است. نتایج حاصل‌شده با نتایج پژوهش‌های اسکینر و فریم[1] (1997)، مک‌کومبز[2] (2008)، بلگورسو و همکاران (2010) و لی و همکاران (2010) همسوست. در تبیین این فرض می‌توان گفت خودکنترلی در افراد سبب رفتار آگاهانه و کنترل‌شده می‌شود. ارائهٔ اینگونه رفتارها از فرد نشان‌دهندهٔ آگاهی او از شرایط و نتایج هر عمل است که دربارهٔ رفتارهای انحرافی و پرخطر، آگاهی از نوع و شدت مجازات می‌تواند سبب جلوگیری از انجام آنها شود. باید در نظر داشت نداشتن خودکنترلی افراد جامعه می‌تواند نقش مهمی در نقض امنیت اطلاعات ایفا و سلامت روانی دیگران را تهدید کند که جبران آن گاهی ماه‌ها و سال‌ها طول می‌کشد. براساس نتایج پژوهش پیشنهاد می‌شود سیاست‌های شدت و حتمیت برخورد با افراد ناقض سیاست‌های امنیت اطلاعات اجرایی و آشکارا پیگیری شوند.

مانند دیگر مطالعات پژوهشی، این مطالعه نیز محدودیت‌های زیر را دارد: ۱- یافته‌های پژوهش تنها به مدت زمان جمع‌آوری داده‌ها و اعتبار آنها به دورهٔ زمانی کوتاه‌مدت محدود است و ممکن است،گذشت زمان بر متغیرهای مطالعه‌شده دراین پژوهش تأثیر بگذارد و سبب تغییر نتایج شود. ۲- یافته‌ها در زمینهٔ سازمان مطالعه‌شده استنادپذیر است و تعمیم‌پذیر به کل جامعه نیست. در این راستا پیشنهاد می‌شود الگوی ارائه‌شده در جوامع آماری دیگر نیز مطالعه شود. همچنین پیشنهاد می‌شود نقش تعدیلگر عوامل بازدارندگی و فرهنگ کارمندان در قصد رعایت یا نقض امنیت اطلاعات مطالعه شود. پیشنهاد می‌شود پژوهشگران با استفاده از نظریه‌های دیگر مانند نظریهٔ یادگیری اجتماعی و نظریه‌های عمومی‌جرم‌شناسی، سعی در بسط الگو داشته باشند.

[1] Skinner & Fream
[2] McCombs

منابع

احمدی‌جزئی، م. (۱۳۹۵). *بررسی فرهنگ سازمانی و تأثیر آن بر مدیریت امنیت اطلاعات*، پایان‌نامهٔ کارشناسی‌ارشد، دانشگاه غیرانتفاعی خرمدره.

اسفندیارپور، الف. (۱۳۸۹). *عوامل مؤثر بر پذیرش سیاست های امنیت اطلاعات توسط کارمندان در سازمان*، پایان‌نامهٔ کارشناسی‌ارشد رشتهٔ مدیریت فناوری اطلاعات، دانشکدهٔ حسابداری و مدیریت، دانشگاه علامه طباطبایی.

بوستانی، د. (۱۳۹۱). «سرمایهٔ اجتماعی و رفتار پرخطر؛ نمونهٔ مورد مطالعه: دانش‌آموزان دبیرستانی شهر کرمان»، *مجلهٔ علوم اجتماعی دانشگاه فردوسی مشهد*، س ۹، ش ۱، ص ۳۱-۱.

بیرو، آ. (۱۳۷۵). *فرهنگ علوم اجتماعی*، ترجمهٔ باقر ساروخانی، تهران: کیهان.

پورنقدی، ب. (۱۳۹۷). «فرصت‌ها و تهدیدهای امنیت در شبکه‌های اجتماعی مجازی برای دانشجویان»، *پژوهش‌های راهبردی امنیت و نظم اجتماعی*، س ۷، ش ۲، ص ۸۹-۸۷.

حسن‌زاده، م.؛ کریم‌زادگان، د. و مقدم‌جهانگیری، ن. (۱۳۹۱). «ارائهٔ یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران»، *نظام‌ها و خدمات اطلاعاتی*، س ۱، ش ۲، ص ۱۶-۱.

حیدری‌ساربان، و. (۱۳۹۶). «تبیین رابطهٔ سرمایهٔ اجتماعی با احساس امنیت اجتماعی ساکنان مناطق روستایی شهرستان مشگین‌شهر»، *پژوهش‌های راهبردی امنیت و نظم اجتماعی*، س ۶، ش ۲، ص ۴۵-۶۲.

خواجویی، ح. (۱۳۹۰). *بررسی کنترل‌های امنیت اطلاعات*، پایان‌نامهٔ کارشناسی‌ارشد در رشتهٔ مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیکی، دانشگاه سیستان و بلوچستان.

سادوسکای، ج.؛ اکس، د. ج. و گرینبرگ، آ. (۱۳۸۴). *راهنمای امنیت فناوری اطلاعات*، ترجمهٔ: مهدی میردامادی، زهرا شجاعی و محمدجواد صمدی، تهران: شورای عالی اطلاع‌رسانی.

سجادی، ع. (۱۳۸۵). «خودکنترلی در نظام کنترل و نظارت اسلامی (با نگاهی بر جایگاه خودکنترلی در نظریه‌های مدیریت)»، *اندیشهٔ صادق*، ش ۲۳، ص ۱۶-۳.

سلیمی، ع. و داوری، م. (۱۳۸۰). *جامعه‌شناسی کجروی*، قم: پژوهشگاه حوزه و دانشگاه.

عباس‌زاده، م.؛ علیزاده‌اقدم، م. و پریزادبنام، ش. (۱۳۹۶). «مطالعهٔ تأثیر هوش هیجانی بر رفتارهای پرخطر عمدی رانندگان»، *پژوهش‌های راهبردی امنیت و نظم اجتماعی*، د ۶، ش ۲، ص ۱۶-۱.

کریمی، ز. و پیکری، ح. (۱۳۹۷). «تأثیر ادراک پرستاران از آموزش امنیت اطلاعات و آگاهی از سیاست‌های امنیت اطلاعات بر ادراک از شدت و قطعیت مجازات نقض امنیت اطلاعات؛ موردمطالعه: بیمارستان‌های تخصصی آموزشی شهر اصفهان»، *آموزش پرستاری*، د ۷، ش ۲، ص ۴۰-۳۱.

نخعی، آ. و خیری، ب. (۱۳۹۱). «بررسی تأثیر عوامل منتخب بر قصد خرید محصولات سبز»، *مجلهٔ مدیریت بازاریابی*، ش ۱۵، ص ۱۳۰-۱۰۵.

ولی، ح. (۱۳۹۱). *شناسایی و اولویت‌بندی عوامل مؤثر بر پذیرش و توسعهٔ سیاست‌های امنیت اطلاعات در سازمان*، پایان‌نامهٔ کارشناسی‌ارشد در رشتهٔ مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیکی، دانشگاه سیستان و بلوچستان.

ویلیامز، ف. و مک‌شین، م. (۱۳۹۱). *نظریه‌های جرم شناسی*، ترجمهٔ: حمیدرضا ملک‌محمدی، تهران: میزان.

Andreoni, J. Harbaugh, W. & Vesterlund, L. (2003) "The Carrot or the Stick: Rewards, Punishments and Cooperation." *The American Economic Review*, 93: 893-902.

Information Research, Chapter in Now or Later: Economic and Psychological Perspectives on Intertemporal Choice. edited by Roy Baumeister, George Loewenstein & Daniel Read. New York, US: Russell Sage Foundation Press.

Park, E. Kim, J. & Park, Y. S. (2017) "The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information." *Computers & Security*, 65: 64-76.

Prinsley, R. Beavis, A. S. & Clifford-Hordacre, N. (2016) *Women in STEM: A Story of Attrition Datasheet*. Canberra: Office of the Chief Scientist.

Siegel, L. J. (2001) *Criminology: Theories, Patterns and Typologies, Massachusetts*. US: University of Massachusetts.

Song, Y. Lee, M. Jun, Y. Lee, Y. Cho, J. & Kwon, M. (2016) "Revision of the Measurement Tool for Patients' Health Information Protection Awareness." *Healthcare Informatics Research,* 22 (3): 206–216

Skinner, W. F. & Fream, A. (1997) "A Social Learning Theory Analysis of Computers Crime among College Students*." Journal of Research Crime Delinquency*, 34 (4): 495-518.

Siponen, M. Pahnila, S. & Mahmood, M. A. (2010) "Compliance with Information Security Policies: An Empirical Investigation." *Computer*, 43 (2): 64-71.

Straub, D. W. & Welke, R. J. (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making." *MIS Quarterly*, 22 (4): 441-469.

Straub, D. W. (1990) "Effective is Security: An Empirical Study." *Information Systems Research,* 1 (3): 255-276.

Subramaniam, C. Park, S. & Kumar, R. L. (2008) "Understanding the Value of Countermeasure Portfolios in Information Systems Security." *Journal of Management Information Systems*, 25 (2): 241-280.

Thomas, H. & Anderson, N. (2006) "Changes in New Comers' Psychological Contracts During Organizational Socialization: A Study of Recruits Entering the British Army." *Journal of Organizational Behavior*, 19: 745-767.

Veiga. A. & Martins, N. (2017) "Defining and Identifying Dominant Information Security Cultures and Subcultures." *Computers & Security*, 70: 72-94.

Von Solms, R. (2014) "Information Security Management (1): Why Information Security is so Important. Information Management and Computer Security." *Journal of Association Information Systems*, 6: 174-177.

Bulgurcu, B. Cavusoglu, H. & Benbasat, I. (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *Management Information Systems*, 34: 523-548.

Chang. E. (2007) "An Investigation of Organizational Culture on Information Security Management." *Academy of Management Journal*, 35: 421-438.

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 Researh*, 20 (1): 79-98.

D'Arcy, J. & Herath, T. (2011) "A Review and Analysis of Deterrence Theory in the is Security Literature: Making Sense of the Disparate Findings." *European Journal of Information Systems*, 20 (6): 643-658.

Fehr, E. & Schmidt, K. M. (2007) "Adding a Stick to the Carrot? The Interaction of Bonuses and Fines." *The American Economic Review*, 97: 177-181.

Ifinedo, P. (2014) "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence and Cognition." *Information Management*, 51 (1): 69-79.

Hu, Q. Xu, Z. Dinev, T. & Ling, H. (2011) "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?" *Communication of the ACM*, 54 (6): 54-60.

Krishnan, R. (2003) "CISSP-Whitepaper Information Security Management Systems." *Information Systems Research*, 1 (3): 255-276.

Kruger, H. A. & Kearney, W. D. (2006) "A Prototype for Assessing Information Security Awareness." *Computers & Security*, 25: 289-296.

Li, H. Zhang, J. & Sarathy, R. (2010) "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory." *Decision Support Systems*, 48 (4): 635-645.

McCombs, B. L. (2008) "Self-Regulated Learning and Academic Achievement: A Phenomenological View." in: Zimmerman, B. J. & Schunk, D. H. (Eds.), *Self-Regulated Learning and Academic Achievement: Theoretical Perspectives*. Oxfordshire, UK: Routledge. 63-118.

Mikko, S. Mahmood, M. A. & Seppo, P. (2014) "Employees' Adherence to Information Security Policies: An Exploratory Field Study." *Information & Management*, 51: 217-224.

O'Donoghue, T. & Rabin, M. (2001) *Healthcare*