فصل‌نامه مطالعات مالی و بانکداری اسلامی
مؤسسه عالی آموزش بانکداری ایران
دوره ۷، شماره ۱۶
بهار و تابستان، ۱۴۰۱
صفحه ۷۷-۹۸

سیاست‌های امنیت اطلاعات: نقش غیرمستقیم حمایت مدیریتی در رفتار انطباقی کاربران سیستم‌های اطلاعاتی بانک‌ها

نادر هاشم‌زاده اقدم [۱]

چکیده

تاکنون در حوزه امنیت اطلاعات سازمانی پژوهش‌های متعددی انجام شده است، اما در پژوهش پیش رو با استفاده از سیاست‌های امنیت اطلاعات در راستای ایمن‌سازی رفتار کاربران سیستم‌های اطلاعاتی از جانب حمایت مدیریتی تلاش شده است. بر همین اساس، پژوهش حاضر با هدف بررسی تأثیرات غیرمستقیم حمایت مدیریتی از طریق نقش میانجی اعتماد درک‌شده و خودکارآمدی بر رفتار انطباقی کاربران با استفاده از سیاست‌های امنیت اطلاعات در یک نمونه تصادفی ۲۵۶ نفری از کارکنان بانک‌های استان آذربایجان شرقی در سال ۱۳۹۸ طراحی و انجام شده است. نتایج مدل‌سازی معادلات ساختاری نشان داد که بر اساس پاسخ شرکت‌کنندگان پژوهش، اعتماد درک‌شده و خودکارآمدی در نقش میانجی، تأثیر حمایت مدیریتی را بر رفتار انطباقی کاربران اعمال می‌کنند. مدل پژوهشی مبتنی بر نظریه رفتار برنامه‌ریزی‌شده، با اتخاذ از یک رویکرد چندبعدی تعاملات بین مدیریت و کاربران را بررسی کرده و در سازگاری رفتار کاربران نقش مهمی ایفا کرده است. همچنین این پژوهش تأثیر حمایت مدیریتی (آموزش، رفتار و تمرین‌دهی رهبر) در راستای منطبق‌سازی رفتار کاربران را برجسته کرده و در خصوص نقش به‌کارگیری سیاست‌های امنیت اطلاعات بحث کرده است.

واژه‌های کلیدی: الگوی امنیت اطلاعات سازمان، حمایت مدیریتی، اعتماد درک‌شده، خودکارآمدی، رفتار انطباقی کاربران، سیاست‌های امنیت اطلاعات.

طبقه‌بندی JEL: L۵۲ و M۱۲.

---

۱. کارشناس ارشد تحقیقات آموزشی، واحد شبستر، گروه علوم تربیتی، دانشگاه آزاد اسلامی، شبستر، شبستر، ایران؛
nader_hashemzade70@yahoo.com

مقدمه

تداخل‌های انجام‌شده در سیستم‌های امنیت اطلاعاتی، با عملکردهای انسانی نسبت به شکست‌های فیزیکی ارتباط قوی دارند (ناریانا سامی، احمد و اسماعیل[1]،۲۰۱۰). میزان امنیت سیستم‌ها در هر سازمان به رفتار امن کاربران وابسته است (راهی، کیم و ریو[2]، ۲۰۰۹). رفتار پذیرفته‌نشده کاربران اغلب به‌عنوان خطای انسانی شناخته می‌شود (العمری، الگایار و دکار[3]، ۲۰۱۲) که می‌تواند به‌عنوان تغییر در عملکرد انسان تعریف شود، باعث انحراف از مسیر موفقیت دل‌خواه شده و به نتیجه ناخواسته یا غیر برنامه‌ریزی‌شده منجر شود (وود و بنکز[4]، ۱۹۹۳: ۵۲).

پژوهش‌های زیادی خطای انسانی را مسئله اصلی در امنیت سیستم‌های اطلاعاتی یافته‌اند (آخوندزاده و همکاران[5]، ۲۰۱۵ و نارایانا سامی و همکاران، ۲۰۱۰). خطای انسانی می‌تواند ریسک امنیتی بالایی را مطرح کند. این در صورتی است که سازمان قادر به کنترل و مدیریت اطلاعات از طریق پیاده‌سازی خط‌مشی‌های امنیت اطلاعاتی نباشد (اهلان، ارشد و لوبیس[6]، ۲۰۱۱). پژوهش‌های زیادی وقایع امنیت اطلاعاتی در سازمان‌ها را گزارش داده‌اند که ۸۰ درصد موارد شکست‌ها به رفتار کاربران نسبت داده می‌شوند که این میزان نرخ ناکامی‌های امنیتی به‌رغم سرمایه‌گذاری زیاد روی راه‌حل‌های امنیتی مبتنی بر فناوری، هنوز هم به رشد خود ادامه می‌دهد (العمری و همکاران[7]، ۲۰۱۲). به بیان ناریانا سامی و همکاران (۲۰۱۰)، خطای انسانی تهدید عمده‌ای برای حفاظت از اطلاعات سازمانی است. برای مثال، گزارش سمنتیک[8] (۲۰۱۳) حاکی از آن است که بخش مراقبت‌های بهداشتی از بالاترین درصد اتفاقات امنیتی برخوردار بوده است. موارد امنیت اطلاعاتی در بخش مراقبت بهداشتی مرتبط با ناآگاهی امنیتی در میان کارکنان، ضعف مهارت‌های امنیتی و کنترل ضعیف اجرای رفتارهای امنیتی بوده‌اند (داویگا و مارتینز[9]، ۲۰۱۵ و صفا، وان سولمز و فورنل[10]، ۲۰۱۶). بنابراین، دولت‌ها و مدیریت صنعت سازمانی به‌طور کلی باید نه‌تنها در جنبه‌های فنی سیستم‌های امنیتی، بلکه در رابطه با ایمن‌سازی رفتارهای منابع انسانی نیز سرمایه‌گذاری کنند.

1. Narayana Samy, Ahmad & Ismail
2. Rhee, Kim & Ryu
3. Al-Omari
4. Wood and Banks Jr
5. Akhunzada et.al
6. Ahlan, Arshad & Lubis
7. Al-Omari, El-Gayar & Deokar
8. Symantec
9. Da Veiga & Martins
10. Safa, Von Solms & Furnell

سیستم اطلاعاتی بانک‌ها باید به‌عنوان یک سیستم اطلاعاتی مالی، از حیث دسترسی‌های غیرمجاز به‌منظور حفاظت و صیانت از اموال ذی‌نفعان از امنیت بالایی برخوردار باشد و کاربران سیستم‌های اطلاعاتی ضمن رعایت اصول امنیتی سیستم‌ها، رفتار صحیح حفاظت از اطلاعات را نهادینه کنند.

واضح است که سازمان‌های مالی و اطلاعاتی که در مواجهه با حفاظت اطلاعات مشتریان و ذی‌نفعان خود اهمیت پررنگی دارند، در راستای مدیریت تأمین امنیت دارایی‌های اطلاعاتی خود، به‌منظور مبارزه با شکست اطلاعاتی، پیش‌بینی‌ها و سیاست‌های لازم را تدبیر کنند. در پژوهش حاضر پژوهشگر به‌منظور منطبق‌سازی رفتار کاربران سیستم‌های اطلاعاتی بانک‌ها با سیاست‌های امنیت اطلاعات، نقش غیرمستقیم حمایت مدیریتی را از طریق دو متغیر میانجی اعتماد درک‌شده و خودکارآمدی بررسی کرده است.

مبانی نظری

رفتار انطباقی سیاست‌های امنیت اطلاعات

گئو[1] (۲۰۱۳) رفتار انطباقی سیاست‌های امنیت اطلاعاتی را به‌عنوان رفتارهایی که سیاست‌های امنیت اطلاعات سازمان را نقض نمی‌کنند، تعریف می‌کند. این رفتارها به مجموعه‌ای از فعالیت‌های امنیتی اطلاق می‌شود که به اصول سازمانی پایبند هستند (پادایاچی[2]، ۲۰۱۲). سیاست امنیت اطلاعات سازمان معمولاً بر چند حوزه مانند مدیریت رمز عبور، مدیریت اطلاعات، کاربرد اینترنت، کاربرد سیستم‌های شبکه اجتماعی و گزارش حوادث متمرکز است (پارسونز و همکاران[3]، ۲۰۱۴).

رفتارهای انطباقی اطلاعات ممکن است بر موفقیت یا شکست فرایندهای امنیت اطلاعات در سازمان‌ها، به‌خصوص در صنعت بانکداری تأثیر بگذارد. بنابراین، ارتقای رفتار امنیتی اطلاعات و محدود کردن رفتار پذیرفته‌نشده امنیت اطلاعات در میان کارکنان برای سازمان‌ها از اهمیت ویژه‌ای برخوردار است (وودهاوس[4]، ۲۰۰۷). در نتیجه، اگر رفتار سازمانی کارمندان در خصوص امنیت اطلاعات پذیرفته شده باشد، حوادث امنیتی می‌تواند به حداقل برسد و کارایی سیاست‌های امنیت اطلاعات افزایش یابد.

---

1. Guo
2. Padayachee.
3. Parsons, Mccormac & Butavicius
4. Woodhouse

نظریه رفتار برنامه‌ریزی‌شده

نظریه رفتار برنامه‌ریزی‌شده[۱]، توسط پژوهشگران برای توضیح رفتار کاربر در رابطه با سیستم‌های اطلاعاتی ارائه و به‌کار برده شده است (یوفن و بریتنر[۲]، ۲۰۱۳). نظریه رفتار برنامه‌ریزی‌شده به‌طور گسترده‌ای برای پیش‌بینی رفتار انسان طراحی شده تا پذیرش کاربران از سیستم اطلاعاتی را بررسی کند (لیائو و همکاران[۳]، ۲۰۰۷). این نظریه پیشنهادشده توسط آزجان[۴] (۱۹۸۵) سه عامل مفهومی مستقل پیش‌بینی‌کننده قصد را مطرح می‌کند: نگرش، هنجارهای ذهنی[۵] و کنترل رفتار درک‌شده[۶]. آزجان (۱۹۸۵) نگرش را به‌عنوان «درجه‌ای که شخص با توجه به آن ارزیابی مطلوب یا نامطلوب یا تأیید رفتار مد نظر را تعریف می‌کند»، بیان کرده است. در عین حال، هنجارهای ذهنی توسط نظرهای کاربران راجع به دیدگاه‌های دیگران (ناظران و رهبران) از نظر اینکه آیا ایشان باید رفتار مناسب را اتخاذ کنند، تعیین می‌شوند (هوانگ و چوانگ[۷]، ۲۰۰۷). با این حال، در این پژوهش، تنها رفتار افراد مافوق برجسته شده است، زیرا رفتار کارکنان در سازمان‌ها اغلب تحت‌تأثیر رهبران خود قرار می‌گیرند که همچنین رهبران سازمان مانند مدیر، ناظر و سرپرست هستند. یافته‌های پژوهش‌های پیشین نشان می‌دهد که رفتار مافوق، در رفتار امنیتی اطلاعات کارمندان بیشترین تأثیر را دارد (هوانگ و چوانگ، ۲۰۰۷ و ایفندو[۸]، ۲۰۱۲). رهبران باید رفتارهای مثبت امنیتی را نشان دهند و کارمندان را برای اجرای رفتارهای منطبق با سیاست‌های امنیتی تشویق کنند (سیپونن، محمود و پانیلا[۹]، ۲۰۱۴). بنابراین، بر حسب پژوهش‌های انجام‌شده می‌توان ادعا کرد که فرهنگ امنیتی مناسب می‌تواند در سازمان‌ها ارتقا یافته و سطح امنیتی اطلاعات را به‌طور مؤثر افزایش دهد.

کنترل رفتار درک‌شده: از دیدگاه تئوری رفتار برنامه‌ریزی‌شده، کنترل رفتار درک‌شده را می‌توان به‌عنوان درک کاربران از توانایی خود توصیف کرد (هوانگ و همکاران[۱۰]، ۲۰۱۱) که می‌تواند از

1. The theory of planned behaviour
2. Uffen & Breitner
3. Liao
4. Ajzen
5. Subjective norms
6. Perceived behavioural control
7. Huang & Chuang
8. Ifinedo
9. Siponen, Mahmood & Pahnila
10. Huang et.al

طریق آموزش‌های ارائه‌شده توسط مدیریت برجسته یابد. بر اساس نظر تیلور و تاد[1] (۱۹۹۵)، ساختار کنترل رفتار درک‌شده دارای دو جزء خودکارآمدی و تسهیل شرایط است.

خودکارآمدی: یکی از عواملی است که تصور می‌شود رفتار انطباقی با سیاست‌های امنیتی را ترویج می‌کند (بولگرکو، کاوسوگلو و بنباست[2]، ۲۰۱۰) که می‌تواند از طریق کسب دانش توسعه یابد (چان، وون و کانکانهیل[3]، ۲۰۰۵). ساختار خودکارآمدی از نظریه شناختی اجتماعی (جانستون و وارکنستین[4]، ۲۰۰۸) می‌آید و تعیین می‌کند که چگونه مردم احساس و فکر می‌کنند و به آنها انگیزه می‌دهد که به‌نحوی خاص، بر مبنای فرایندهای شناختی، انگیزشی، عاطفی، نفوذ و انتخاب اجتماعی رفتار کنند (ورکمن، بامر و استروب[5]، ۲۰۰۸). پژوهشگران این موضوع را که خودکارآمدی می‌تواند از طریق برنامه‌های آموزشی ارائه‌شده توسط مدیریت تقویت شود، تأیید کرده‌اند (بیلز و سالانوا[6]، ۲۰۰۶). خودکارآمدی مرتبط با رعایت قوانین مربوط به امنیت اطلاعاتی، نه‌تنها استفاده مناسب از اقدامات متقابل امنیتی را در بر می‌گیرد، بلکه شامل رفتارهای مراقبت امنیتی مربوط به استفاده از رایانه یا اینترنت نیز می‌شود.

شرایط تسهیل: شرایط تسهیل که مؤلفه دوم کنترل رفتار درک‌شده است، به تسهیلات مورد نیاز برای تضمین اینکه کارکنان در رفتارهایی که سازمان از آنها می‌خواهد (مانند پول، زمان و منابع تخصصی) مشارکت دارند، مرتبط است (تیلور و تاد، ۱۹۹۵). برنامه‌های آموزشی می‌توانند آگاهی امنیت اطلاعات کاربران را توسعه داده (پوهاکاینین و آهونن[7]، ۲۰۰۶) و مهارت آنها را برای استفاده از ابزارهای امنیتی تقویت کنند (کوسکوساس، کاکیولیدز و سیاموس[8]، ۲۰۱۱) که به بهبود رفتار انطباق کاربران با سیاست‌های امنیت اطلاعات منجر می‌شود. پژوهشگران معتقدند که تعهد کامل و حمایت از کارکنان در به‌کارگیری بهترین شیوه‌های رفتار امنیت اطلاعاتی، در موضوع مدیریت بسیار حائز اهمیت است و چنین تظاهراتی در سطح بالا می‌تواند آگاهی کاربران از امنیت اطلاعات را تحت‌تأثیر قرار دهد.

---

1. Taylor & Todd
2. Bulgurcu, Cavusoglu & Benbasat
3. Chan, Woon & Kankanhalli
4. Johnston & Warkentin
5. Workman, Bommer & Straub
6. Beas & Salanova
7. Puhakainen & Ahonen
8. Koskosas, Kakulidis & Siomos

اعتماد به سازمان

به بیان بریدی[1] (۲۰۱۱)، اعتماد به سیاست‌های امنیت اطلاعات می‌تواند انطباق با سیاست‌ها را میان کارکنان بهبود بخشد. از دیدگاه روان‌شناختی، اعتماد به‌صورت تمایل فرد (یا اعتمادکننده) به پذیرش آسیب نسبت به عملکرد فرد دیگر (فرد مورد اعتماد) تعریف می‌شود (مک درومت و همکاران[2]، ۲۰۱۳ و شهنواز و گوسوامی[3]، ۲۰۱۱) که بر اساس آن، فرد بر این باور است که او از افراد دیگر سود نمی‌برد (سیکس و سورگ[4]، ۲۰۰۸). راهی[5] (۲۰۱۰) اعتماد را به‌عنوان ساختار سه‌بعدی دسته بندی کرده است: الف. اعتماد اجتماعی که در فرهنگ اجتماعی منعکس شده، ب. اعتماد سازمانی که با عنوان درجه اعتماد سازمان تعریف شده (منعکس‌کننده قوانین کاری و هنجارهای فعالیت‌های کاری در سازمان‌ها) و ج. اعتماد به دیگران، رابطه اعتمادی بین همکاران و کارفرمایان. بر اساس نظر تان و لیم[6] (۲۰۰۹)، اعتماد به سازمان به تمایل کارکنان به آسیب‌پذیر بودن نسبت به اقدامات سازمان اشاره دارد و مشخص شده که عامل مهمی در انگیزش تعهد کارمند و افزایش عملکرد سازمانی است (کلپ و ییلمازتورک[7]، ۲۰۱۲ و هوگلر، هنل و گروس[8]، ۲۰۱۳).

اوتامی، بانگون و لانتو[9] (۲۰۱۴) این یافته را تأیید کردند و بر اهمیت کسب اعتماد کارکنان توسط سازمان به‌منظور افزایش تعهد کاری تأکید داشتند. به گفته شهنواز و گوسامی (۲۰۱۱)، عامل تعهد در ساخت روابط انسانی مهم است که در این مورد، رابطه بین کارفرما و کارمند مد نظر است. اگر کارکنان احساس کنند که کارفرما به‌خوبی با آنها رفتار می‌کند، برای رسیدن به اهداف سازمانی سخت‌تر تلاش خواهند کرد و تعهدات آنها به سازمان نیز افزایش می‌یابد (کلپ و ایلمازتورک، ۲۰۱۲). پژوهش‌های تجربی گزارش داده‌اند که اعتماد، بر رفتار مشتریانی که قصد تجارت آنلاین دارند، تأثیری مثبت دارد (کیم و همکاران[10]، ۲۰۱۰) و شاخص پیش‌بینی قدرتمندی از رفتار امنیت اطلاعاتی میان کارکنان است (ویلیامز[11]، ۲۰۰۸). در محیط سازمان‌ها، کارکنان باید هنگام برخورد با

1. Brady
2. Mcdermott, Conway & Rousseau
3. McDermott, Shahnawaz & Goswami
4. Six and Sorge
5. Rhee
6. Tan & Lim
7. Celep & Yilmazturk
8. Hogler, Henle & Gross
9. Utami, Bangun & Lantu
10. Kim, Tao, Shin, Kim
11. Williams

داده‌های سازمانی تعهد کامل داشته باشند (بریدی، ۲۰۱۰)، به‌ویژه زمانی که این داده‌ها در معرض شبکه‌ای آسیب‌پذیر قرار دارد و خطری برای امنیت اطلاعات به وجود می‌آورد (ون دورسن[1]، ۲۰۱۳). ریسک‌های احتمالی امنیت عبارت‌اند از: اشتراک‌گذاری رمزهای عبور کارکنان برای دسترسی به داده‌های اطلاعات، ترک رایانه بدون خروج از سیستم، ارسال اطلاعات کارکنان و مراجعان به مخاطبان دیگر که به این ترتیب اطلاعات ذی‌نفعان را به کاربران غیرمجاز افشا می‌کنند. خطرهای بالقوه ناشی از درک نکردن مفاهیم امنیتی در میان کارکنان است و این به نفع اعتماد در محیط کاری است، نه اعتماد به سیاست‌های امنیتی (ویلیامز، ۲۰۰۹). با توجه به این موضوع، اعتقاد بر این است که اعتماد به سازمان‌ها باید بین کارمندان و مدیریت سازمان تعبیه شود تا کارمندان به پیروی از امنیت اطلاعاتی که در اختیار دارند، بیشتر متعهد شوند. در پژوهش حاضر بر عوامل سازمانی مانند اجرای سازوکارهای امنیتی، آموزش امنیت اطلاعات و پیاده‌سازی سیاست‌های امنیت اطلاعات تمرکز شده است، در حالی که نظارت و آموزش کارکنان برای رفتار مناسب در رابطه با امنیت اطلاعات به‌عنوان جنبه‌های حمایت مدیریتی در نظر گرفته شده‌اند.

حمایت مدیریتی، خودکارآمدی و رفتار انطباقی کاربران

حمایت مدیریتی به‌صورت درک کاربران از تعهد بالای مدیریتی به‌منظور حفاظت اطلاعات توصیف شده که این یکی از جوانب در مؤلفه‌های بحران امنیتی است (داویگا و الوف[2]، ۲۰۱۰). الصالحی، آن و سورس[3] (۲۰۰۳) حمایت مدیریتی را به‌عنوان تعهدی از مدیریت در سازمان به‌صورت مشاهده‌شده توسط کاربران تعریف کرده‌اند. پشتیبانی کامل از مدیریت در هر سازمان برای تضمین بازده امنیت سیستم اطلاعات و توانمندسازی خلق محیطی امن برای اداره اطلاعات ضروری است (بریدی، ۲۰۱۱ و هو و همکاران[4]، ۲۰۱۲). در محیطی امن، این تعهد به مستندسازی سیاست‌های امنیت اطلاعات سازمان اشاره دارد و حصول اطمینان از اینکه سیاست‌ها و رویه‌های سازمانی در حال اجرا و برنامه‌های آموزش آگاه‌سازی انجام می‌گیرد (کناپ و همکاران[5]، ۲۰۰۹). با توجه به نظر کانکانهالی و همکاران[6] (۲۰۰۳)، حمایت مدیریتی به‌عنوان شکلی از هدایت و رهنمود در نظر گرفته می‌شود که

1. Van Deursen, Buchanan & Duff
2. Da Veiga & Eloff
3. Al-Salihy, Ann & Sures
4. Hu, Dinev, Hart & Cooke
5. Knapp, Franklin, Morris & Marshall
6. Kankanhalli, Teo, Tan & Wei

طی برنامه‌ریزی و پیاده‌سازی امنیت اطلاعاتی ارائه شده است. مطالعات تجربی نیز اهمیت حمایت مدیریتی را ثابت کرده است. بریدی (۲۰۱۱) در پژوهش خود نشان داد که حمایت مدیریتی شاخص پیش‌بینی شایان توجهی از رفتار امنیتی متخصصان مراقبت‌های بهداشتی نسبت به قانون حمل‌ونقل و حسابرسی بیمه در ایالات متحده است.

در پژوهش حاضر، خودکارآمدی به‌عنوان درک فرد از قابلیت خود برای حفاظت اطلاعاتی تعریف شده است (جانستوون و وارکنتین[1]، ۲۰۰۸). خودکارآمدی می‌تواند از طریق برنامه‌های آگاهی امنیت اطلاعاتی و آموزش تقویت شود که هدف آن معرفی و تهیه اطلاعات درباره اهمیت امنیت سیستم‌های اطلاعاتی و افزایش مهارت‌های کاربران در استفاده از معیار امنیتی است (ترکزاده و ون دایک[2]، ۲۰۰۲). کاربران ممکن است از تهدیدهای امنیت اطلاعاتی آگاه شده و دانش خوبی درباره معیارهای امنیتی داشته باشند، اما چنانچه مهارت آنها در رویارویی با این تهدیدها ضعیف باشد، احتمال کمتری در پیاده‌سازی معیارهای امنیتی پیشگیرانه خواهند داشت (ورکمن و همکاران، ۲۰۰۸). از این رو، مدیریت باید به کارکنان درباره نحوه استفاده از معیارهای امنیتی به‌طور مناسب و بیان علت حفظ رفتار مؤثر امنیتی در تهدیدهای امنیت اطلاعاتی آموزش دهد. این باور وجود دارد که مهارت کاربران هم در تنظیم معیارهای امنیتی و هم در تعدیل تأثیر حمایت مدیریتی بر رفتار انطباقی نسبت به سیاست‌های امنیت اطلاعات مؤثر باشد.

حمایت مدیریتی بر رفتار انطباقی کاربران نسبت به سیاست‌های امنیت اطلاعات از طریق خودکارآمدی، تأثیری غیرمستقیم دارد. همچنین مشخص شده که خودکارآمدی، از اکتساب مثبت مهارت‌ها میان کارکنان در برخورد با رفتار انطباقی نسبت به سیاست‌های امنیت اطلاعات حمایت به عمل می‌آورد (بیس و سالانوا، ۲۰۰۶ و چان و همکاران، ۲۰۰۵). در پژوهش‌های پیشین مشخص شده است که خودکارآمدی بر مقاصد کاربران برای انطباق به سیاست‌های امنیت اطلاعات سازمان، تأثیر مشخصی دارد (بولگروکو و همکاران،۲۰۱۰ و هراث و رائو[3]، ۲۰۰۹) و این رفتار انطباقی نسبت به سیاست‌های امنیت اطلاعات می‌تواند توسط افزایش خودکارآمدی ترویج شود (چان و همکاران، ۲۰۰۵). پانهیلا، سیپونن و محمود[4] (۲۰۰۷) این موضوع را تأیید می‌کنند که خودکارآمدی در توضیح پایبندی مردم به امنیت سیستم اطلاعاتی مهم بود. کارکنان احتمالاً بیشتر سیاست‌های امنیت

1. Johnston & Warkentin
2. Torkzadeh & Van Dyke
3. Herath & Rao
4. Pahnila, Siponen & Mahmood

اطلاعاتی سازمان خود را می‌پذیرند و چنانچه شایستگی نسبی و قابلیتی با توجه به احتیاطات امنیت اطلاعاتی داشته باشند، معیارهای امنیتی پیشگیرانه را پیاده‌سازی می‌کنند (ایفیندو، ۲۰۱۲).

حمایت مدیریتی، اعتماد درک‌شده و رفتار انطباقی کاربران

اعتماد درک‌شده به سطح اعتماد به نفس کاربران در زمینه پیاده‌سازی سیاست‌هایی از طریق حمایت مدیریتی اشاره دارد. درک و پذیرش اعتماد میان کابران به نیازهای ذهنی و محدودیت‌های اجتماعی کاربران وابسته است. چنانچه کاربران، به سیستم امنیتی اعتمادی بالاتر داشته باشند، احتمالاً به‌طور پیوسته از سیستم امنیتی استفاده خواهند کرد که به‌نوبه خود وقایع امنیتی را در سازمان کاهش می‌دهد (باتیار و لایان[1]، ۲۰۱۳). لیپرت و دیویس[2] (۲۰۰۶) این موضوع را این طور بیان کردند که اعتماد جزء مهمی در سازمان است و بر تمایل کارمند به‌منظور پذیرش امنیت فناوری تجهیزشده در سازمان مؤثر است. با توجه به این موضوع، این باور وجود دارد که اعتماد در سازمان‌ها باید بین کارکنان و مدیریت نهادینه شود، بنابراین کارکنان بیشتر به تطبیق با سیاست‌های امنیت اطلاعاتی پیاده‌سازی‌شده در سازمان متعهد خواهند شد و سوانح و حوادث امنیتی کاهش خواهد یافت.

با توجه به توصیف‌های بیان‌شده فرضیه‌های زیر مطرح می‌شود:

فرضیه ۱. حمایت مدیریتی بر خودکارآمدی، تأثیر مستقیم دارد.

فرضیه۲. حمایت مدیریتی بر اعتماد درک‌شده، تأثیر مستقیم دارد.

فرضیه۳. خودکارآمدی بر رفتار انطباقی کاربران نسبت به سیاست‌های امنیت اطلاعاتی، تأثیری مستقیم دارد.

فرضیه٤. اعتماد درک‌شده بر رفتار انطباقی نسبت به سیاست‌های امنیت اطلاعاتی، تأثیر مستقیم دارد.

فرضیه۵. حمایت مدیریتی بر رفتار انطباقی کاربران به سیاست‌های امنیت اطلاعاتی از طریق اعتماد درک‌شده، تأثیر غیرمستقیم دارد.

فرضیه٦. حمایت مدیریتی بر رفتار انطباقی کاربران به سیاست‌های امنیت اطلاعاتی از طریق خودکارآمدی، تأثیر غیرمستقیم دارد.

---

1. Bahtiyar & layan
2. Lippert & Davis

روش‌شناسی پژوهش

پژوهش حاضر از لحاظ هدف، کاربردی و از حیث روش‌شناسی توصیفی پیمایشی از نوع علی است که در استان آذربایجان شرقی در سال ۱۳۹۸ انجام شده است. جامعه آماری این پژوهش شامل کلیه کارکنان بانک‌های استان آذربایجان شرقی است که از این تعداد ۲۵۶ نفر به شیوه نمونه‌گیری تصادفی طبقه‌ای بر حسب جدول مورگان به‌عنوان نمونه انتخاب شدند و در نهایت تعداد ۲۱۸ پرسش‌نامه بهره‌برداری شدند.

مدل پژوهشی

مدل تطبیق سیاست‌های امنیت سیستم اطلاعاتی به‌منظور استفاده در این پژوهش شامل سه ساختار بیرونی (متغیرهای مستقل)؛ حمایت مدیریتی، خودکارآمدی و اعتماد درک‌شده، بود. ساختار حمایت مدیریتی به‌وسیله رفتار رهبری و پیاده‌سازی تمرین و آموزش سیاست‌های امنیت اطلاعاتی سنجیده شد، در حالی که خودکارآمدی و اعتماد درک‌شده به‌عنوان واسطه در نظر گرفته شدند. ساختار درونی (متغیروابسته) در پژوهش رفتار انطباقی کاربران نسبت به سیاست‌های امنیت اطلاعاتی در جامعه کارکنان بانک‌ها بود.

ابزار گردآوری داده‌ها

ابزار جمع آوری داده در پژوهش حاضر پرسش‌نامه‌ای متشکل از دو بخش بود: بخش نخست شامل پرسش‌های جمعیت‌شناختی مانند جنسیت، سن، تجربه، شغل و نوع سازمان. بخش دوم مربوط به سنجش متغیرها است. شاخص‌های استفاده‌شده برای اندازه‌گیری مدیریت حمایتی از (آرون[1]، ۲۰۰۶؛ میلر، لاند و کوک[2]، ۱۹۹۷ و ان جی، اتری و یانجی[3]، ۲۰۰۹) برای آموزش امنیت اطلاعات و (چانگ، وو و لیو[4]، ۲۰۱۲) برای پیاده‌سازی سیاست امنیت اطلاعاتی اقتباس شده بود. اقلام استفاده‌شده به‌منظور سنجش خودکارآمدی از ایفیندو (۲۰۱۲) و اعتماد درک‌شده از چانگ و کاون (۲۰۰۹) به دست آمدند. تمام شاخص‌ها در بخش‌های دوم و سوم با استفاده از مقیاس پنج‌گانه لیکرت با تغییر از ۱ (کاملاً مخالف) تا ۵ (کاملاً موافق) ارزیابی شدند.

---

1. Aaron
2. Meillier, Lund & Kok
3. Ng, Atreyi & Yunjie
4. Chang, Wu & Liu

ابزار تحلیل داده‌ها

برای تجزیه و تحلیل داده‌ها و بررسی فرضیه‌ها از آمار توصیفی (گرایش‌های مرکزی و پراکندگی) و آمار استنباطی (مدل‌یابی ساختاری) از دو نرم‌افزار اس‌پی‌اس‌اس نسخه ۲۳ و آموس نسخهٔ ۲۴ بهره برده شد.

یافته‌های پژوهش

یافته‌های حاصل از تجزیه و تحلیل داده‌ها به تفکیک در این قسمت گزارش شده است. جدول ۱ اطلاعات توصیفی مربوط به نمونه آماری را که معرف ویژگی‌های شرکت‌کنندگان پژوهش است، نشان می‌دهد.

جدول ۱. اطلاعات توصیفی نمونه آماری

متغیر		فراوانی	درصد فراوانی
جنسیت	مرد	۱۸۵	٪۸۵
	زن	۳۳	٪۱۵
سن	پایین ۴۰	۱۴۶	٪۶۷
	بالای ۴۰	۷۲	٪۳۳
تحصیلات	کارشناسی	۱۷۰	٪۷۸
	کارشناسی ارشد	۴۲	٪۱۹
	دکتری	۶	٪۳
شغل	مدیر	۱۴	٪۶/۵
	کارمند	۲۰۴	٪۹۳/۵
تجربه کاری	زیر ۱۵ سال	۱۲۵	٪۵۷
	بالای ۱۵ سال	۹۳	٪۴۳
نوع بانک	دولتی	۹۵	٪۴۳/۵
	خصوصی	۱۲۳	٪۵۶/۵

اطلاعات توصیفی مربوط به متغیرهای پژوهش در جدول ۲ درج شده است.

جدول ۲. اطلاعات توصیفی متغیرها

متغیر	تعداد پرسش	آلفا	میانگین	انحراف معیار	کمینه	بیشینه
حمایت مدیریتی	۱۷	۰/۸۲	۵۶/۹۰	۱۱/۵۷	۲۲	۸۵
اعتماد درک‌شده	۴	۰/۷۸	۱۳/۳۰	۳/۱۲	۴	۲۰
خودکارآمدی	۴	۰/۸۴	۱۴/۴۳	۲/۹۱	۵	۲۰
رفتار انطباق کاربران	۵	۰/۸۰	۱۶/۳۵	۳/۹۹	۵	۲۵

اطلاعات توصیفی مربوط به متغیرهای پژوهش در جدول ۲ گزارش شده است که همگی در حالت نرمال و قابل قبول قرار دارند.

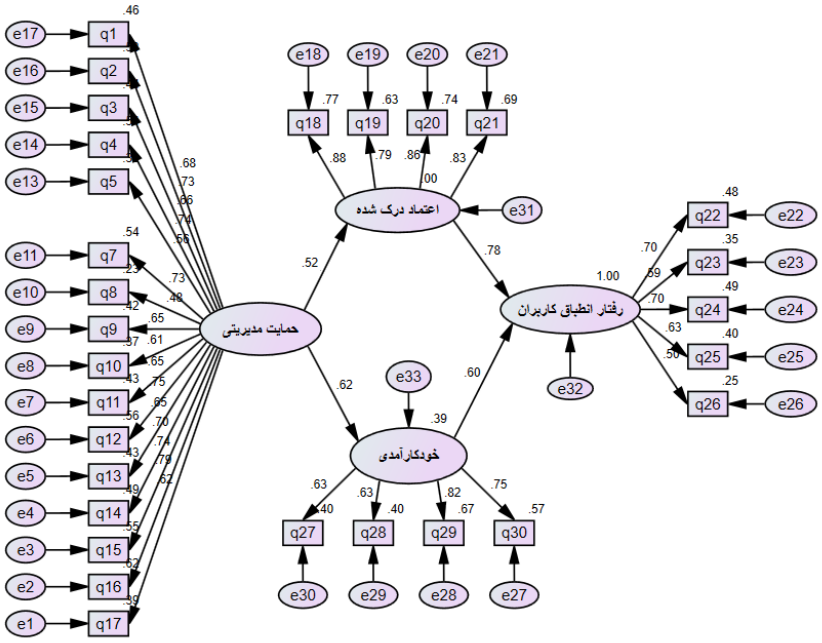
مقادیر هم‌بستگی بین متغیرها در جدول ۳ گزارش شده است که همگی در سطح معناداری قابل قبول به دست آمده‌اند.

جدول ۳. هم‌بستگی بین متغیرها

	حمایت مدیریتی	اعتماد درک‌شده	خودکارآمدی
حمایت مدیریتی	۱		
اعتماد درک‌شده	۰/۷۵**	۱	
خودکارآمدی	۰/۸۶**	۰/۶۶**	۱
رفتار انطباق کاربران	۰/۵۶**	۰/۵۵**	۰/۶۵**

شکل ۱ مدل ساختاری پژوهش را نشان می‌دهد، همچنین در جدول ۴، ضرایب مسیر و سطح معناداری مدل برازش‌یافته درج شده است.

مقادیر ضرایب مسیر و خطای تخمین همراه با سطح معناداری آنها در جدول ۴ گزارش شده است که در حد قابل قبول قرار دارند. گزارش جدول نشان می‌دهد که تراوش واریانس حمایت مدیریتی نسبت به اعتماد درک‌شده و خودکارآمدی کارکنان به‌ترتیب ۰/۲۷ و ۰/۳۸ است. همچنین، اعتماد درک‌شده و خودکارآمدی کارکنان به‌ترتیب به میزان ۰/۶ و ۰/۳۶ واریانس رفتار انطباقی کارکنان را تبیین می‌کنند.



شکل ۱. مدل ساختاری اصلاح‌شده پژوهش

جدول ٤. ضرایب مسیر و سطح معناداری مدل برازش‌یافته

مسیر	ضریب مسیر	R^2	خطای تخمین	مقدار T	معناداری
حمایت مدیریتی ⟵ اعتماد درک‌شده	۰/۵۲	۰/۲۷	۰/۰۵۱	۷/۵۳	۰/۰۰۳
حمایت مدیریتی ⟵ خودکارآمدی	۰/۶۲	۰/۳۸	۰/۰۴۷	۶/۸۲	۰/۰۰۱
اعتماد درک شده ⟵ رفتار انطباقی کاربران	۰/۷۸	۰/۶	۰/۰۱۵	۸/۲۸	۰/۰۰۱
خودکارامدی ⟵ رفتار انطباقی کاربران	۰/۶۰	۰/۳۶	۰/۰۲۸	۷/۳۲	۰/۰۰۱

برازش مدل

با توجه به جدول ۵ تمامی مقادیر به‌دست‌آمده برای فاکتورهای برازش مدل در مقایسه با مقادیر ملاک در حدود قابل قبولی قرار دارند، بنابراین مدل ارائه‌شده در پژوهش حاضر تطابق به نسبت نزدیکی با واقعیت دارد.

جدول ۵. شاخص ملاک برازش هر شاخص و شاخص محاسبه‌شده در پژوهش حاضر

شاخص ها	ملاک برازش	مقادیر به‌دست‌آمده
CFI	>۰/۹۰	۰/۹۴
GFI	>۰/۹۰	۰/۹۱
AGFI	>۰/۸۰	۰/۸۹
RMSEA	<۰/۰۸	۰/۰۵۶
RMSR	<۰/۱۰	۰/۰۴۷
NFI	>۰/۹۰	۰/۹۳

منبع: (هیر و همکاران، ۲۰۱۰ و کلین، ۲۰۱۵)

آزمون سوبل

برای سنجش نقش متغیر میانجی از آزمون سوبل استفاده می‌شود که در جدول ۶ نتایج آزمون سوبل برای متغیرهای میانجی گزارش شده است.

جدول ٦. نتایج آزمون سوبل برای بررسی نقش متغیرهای میانجی

مقادیر/ متغیرهای میانجی	اعتماد درک شده	خودکارآمدی
ضریب رگرسیون مسیر a	۰/۵۲	۰/۶۲
ضریب رگرسیون مسیر b	۰/۷۸	۰/۶۰
خطای استاندارد مسیر a	۰/۰۰۷	۰/۱۲۴
خطای استاندارد مسیر b	۰/۳۱۲	۰/۰۵۹
آماره سوبل	۲/۴۹	۴/۴۸
سطح معناداری	۰/۰۱۲	۰/۰۰۰۰۷۲

با توجه به نتایج جدول ۶ و معناداری مقدار آماره به‌دست‌آمده، نقش میانجی اعتماد درک‌شده و خودکارآمدی در رابطه بین حمایت مدیریتی و رفتار انطباقی کاربران تأیید می‌شود.

بحث

این پژوهش مدل رفتار انسانی را با استفاده از نقش میانجی‌گری اعتماد درک‌شده و خودکارآمدی در زمینه مدیریت امنیت می‌توان معرفی کرد. این ترکیب خاص رفتارهای انسانی، توجه پژوهشگران زیادی را در پژوهش‌های مختلف جهانی به‌سوی خود جلب کرده است، اما به رفتارهای انطباقی

سیاست‌های امنیت اطلاعات در ایران توجه نشده است. این پژوهش، شکاف پژوهشی بین ساختارهای مختلف حمایت مدیریتی و رفتار انطباقی را نیز پر کرده است. اگر چه نقش مدیریت به‌طور گسترده‌ای استفاده نشده، اما به‌منظور ارزیابی ارتباط بین رفتار کارکنان و اثربخشی فناوری در فرهنگ بومی، با توجه به سطح دانش موجود، هیچ یک از پژوهش‌ها به‌طور خاص به ارتباط بین حمایت مدیریتی و اثربخشی امنیت اطلاعات جامعه بانکداری از طریق رفتار انطباقی متمرکز نشده است. این پژوهش بر جنبه‌های مختلف حمایت مدیریتی (آموزش امنیت اطلاعات، رفتار رهبری و تمرین و کنترل آنها) در ارزیابی الگوهای سازگاری رفتار در میان کارکنان بانک‌ها تأکید زیادی دارد. نتایج پژوهش نشان داد که حمایت مدیریتی بیشترین تأثیر را بر اعتماد کارکنان در سیاست‌های امنیتی سازمان دارد. تأثیر اعتماد درک‌شده بر رفتارهای حرفه‌ای امنیتی نسبت به سیاست‌های امنیتی بخش بانکی پیش‌بینی‌کنندگی بیشتری از خودکارآمدی بود که مطابق با نتایج پژوهش‌های قبلی است (ویلیامز، ۲۰۰۸).

بنابراین، مدیریت بانک باید اطمینان حاصل کند که سیاست‌های امنیتی به‌طور مستقیم مستند و بین همه کارکنان توزیع می‌شوند. آموزش‌های سیاست‌های امنیت اطلاعات باید به‌طور اثربخش تدارک شوند تا درک آنان برای کارکنان آسان بوده و در نتیجه بتوانند بر حسب دستورالعمل‌های امنیتی تمرین کرده و در موارد ضروری اقدامات لازم را اعمال کنند. در مقالات پیشین نیز پیشنهاد شده است که ارتباط در خصوص امنیت اطلاعات بین مدیریت و کارکنان باید برای تأثیر بر اعتماد کارکنان مؤثر باشد (کسکوساس و همکاران، ۲۰۱۱). اگر اعتماد بین کارکنان وجود نداشته باشد، بخش اطلاعاتی ممکن است با خطرهای بیشتری از حوادث امنیتی مواجه شود. بنابراین، فرهنگ‌سازی برای ایجاد اعتماد به سازمان باید قبل از اجرای سیاست امنیت اطلاعات در سازمان تعبیه شود. مدیریت در سازمان‌ها در بهبود مهارت‌های امنیتی کارکنان نیز نقش مهمی دارد که مطابق با پژوهش‌های قبلی است (مدهاون و فیلیپس[1]، ۲۰۱۰ و اسپینون و همکاران، ۲۰۱۴). کاربران سیستم‌های اطلاعاتی معتقد بودند که برنامه‌های آموزشی و برنامه‌های آگاهی امنیت اطلاعات مهم و کارساز هستند. به عقیده آنها، آموزش‌های خوب و برنامه‌های آگاهی‌رسانی مؤثر امنیتی می‌توانند نگرش آنها را بهبود بخشند و رفتار آنها را در ارتباط با امنیت اطلاعات تغییر دهند تا مهارت‌های خود را در استفاده از ابزارهای امنیت اطلاعات افزایش دهند. بنابراین، رهبران سازمان‌ها در مدیریت مشکلات ناشی از خطاهای انسانی نقش مهمی ایفا می‌کنند. این نشان می‌دهد که رهبران سازمان‌ها

1. Madhavan & Phillips

باید بیشتر در موضوع آموزش امنیت اطلاعات سرمایه‌گذاری کنند تا اطمینان حاصل شود کـه رفتـار مطلوب امنیت اطلاعات در سازمان‌ها حفظ می‌شود. نقش متغیرهای مداخله (اعتماد و خودکارآمـدی) که در این پژوهش برجسته شده است، تأثیر خود را در رابطه بین حمایت مـدیریتی و رفتـار انطبـاقی کاربران در خصوص سیاست‌های امنیت اطلاعات نشان دادند. نتایج این پژوهش نشان می‌دهـد کـه مدیران بانک ابتدا باید به‌منظور ایجاد یک محیط سازمانی که به اهداف امنیتی منجر می‌شود، اهمیت امنیت اطلاعات را شناسایی کنند. افزون بر این، مدیریت سازمان‌ها باید به‌طور مرتب بـا کارکنـان در ارتباط باشند و مدام با اعمال خود، تداعی‌گر اهداف سازمانی و معیارهای ارتقای شغلی باشند تا از این راه کارکنان از فرصت‌هایی که در اختیار دارند، ادراک درستی داشته و در راستای بازدهی آنان تـلاش کنند.

نتیجه‌گیری

نتیجهٔ تجزیه و تحلیل مدل‌سازی به‌کمک نسخهٔ ۲۲ نرم‌افزار آموس نشان داد کـه تمـام سـازه‌هـای مدل انطباقی، رفتار سازمانی کاربران را نسبت به سیاست‌های امنیتی جامعه بانکی به‌طور مستقیم یـا غیرمستقیم تحت‌تأثیر قرار داده‌اند. این یافته‌ها می‌توانند به رفتـار انسـانی در پـژوهش‌هـای کـاهش اشتباهات رفتاری کمک کرده و برای سیاست‌گذاران در راستای بهبود برنامه‌ریزی استراتژیک مـرتبط با امنیت اطلاعات سازمان‌ها با تأکید بر مسائل مربوط به مدیریت و فاکتورهای انسـانی، بـه‌ویـژه در بخش‌های بانکداری و سازمان‌هایی که به سیستم‌های اطلاعاتی وابسته هسـتند، مفیـد واقـع شـوند. اگرچه اکثر سازمان‌ها زمان و منابع خود را برای ایجاد و حفظ برنامه‌های استراتژیک برای اطمینان از برقراری امنیت اطلاعات سرمایه‌گذاری می‌کنند، اما اگر کارکنـان تمـایلی بـه رفتـار امنیتـی مناسـب نباشند، تلاش‌های آنها بیهوده است. در حالی که تمام ترکیب‌های رفتار اعتماد درک‌شـده بـا عوامـل انسانی در این پژوهش شامل افزایش درک سازگاری رفتار در ارتباط با سیاست‌های امنیت اطلاعـات سازمانی بود، به بیان بهتر خودکارآمدی و اعتماد به‌عنـوان عـواملی مـؤثر شـناخته شـدند. همچنـین آموزش، رفتار و تکرار و تمرین آموزش‌ها که به‌عنوان مؤلفه‌های حمایت مدیریتی در پژوهش حاضـر جا گرفته‌اند، از پراهمیت‌ترین اسـتراتژی‌هـای افـزایش دانـش و مهـارت‌هـای افـراد هسـتند کـه در سازمان‌ها مدیران می‌توانند با تدارکات برنامه‌هـای کارآمـد و متناسـب بـا سـازمان خـود، بهـره‌وری کارکنان خود را در راستای نیل به اهداف متعالی هدایت کنند.

این پژوهش با برجسته‌سازی نقش حمایت مدیریتی در راستای تقویت مهارت رفتار امنیتی کاربران و همچنین با اجرای سیاست‌های امنیت اطلاعات در سازمان، افزایش اعتماد و خودکارآمدی در کارکنان را فراهم آورده و تا حد قابل قبولی سطح ایمنی استفاده از سیستم های اطلاعاتی را بهبود بخشید. به بیان گزیده‌تر، هرچه کاربران سیستم‌های اطلاعاتی سازمان، در رعایت سیاست‌های امنیت اطلاعات کوشا باشند به همان میزان مواجهه با شکست اطلاعاتی تقلیل خواهد یافت.

با توجه به نتایج این پژوهش، سازمان‌های مشابه می‌توانند با اجرای سیاست‌های امنیت اطلاعات و تقویت حمایت مدیریتی دال بر آموزش‌های رعایت اصول امنیت اطلاعات و ارتقای مهارت‌های رفتاری و اعتماد و خودکارآمدی در بین کارکنان سازمان، میزان شکست اطلاعاتی را به میزان چشم‌گیری مدیریت کنند. پژوهش‌های آینده می‌توانند با تمرکز بر سایر عواملی که انگیزش کارکنان را در حفاظت از اطلاعات تقویت می‌کنند یا آموزش‌هایی که از جوانب مختلف رفتار امنیتی کارکنان را حمایت می‌کنند، تدارک دیده شوند.

منابع و مآخذ

Aaron, G.A. (2006). Transformational and transactional leadership: association with attitudes toward evidence-based practice. ***Psychiatric Services,*** 57(8), 1162–1169.

Ahlan, A.R., Arshad, Y. & Lubis, M. (2011). Implication of human attitude factors toward information security awareness in Malaysia Public University. ***Paper presented at International Conference on Innovation and Management,*** 12–15 July, Kuala Lumpur, Malaysia.

Ajzen, I. (1985). From intentions to actions: a theory of planned behavior. ***In: Kuhl J and Beckman J (eds), Action-Control: From Cognition to Behavior.*** Heidelberg: Springer.

Akhunzada, A., Sookhak, M., Anuar, N.B., Gani, A., Ahmed, E., Shiraz, M., Furnell, S., Hayat, A., Khurram Khan, M. (2015). Man-at-theend attacks: analysis, taxonomy, human aspects, motivation and future directions. ***Journal of Network and Computer Applications***, 48: 44–57.

Al-Omari, A., El-Gayar, O. & Deokar, A. (2012). Information security policy compliance: the role of information security awareness. ***Conference: In Proceedings of the 18th Americas Conference on Information Systems (AMCIS 2012).*** At: Seattle, WA.

Al-Salihy, W., Ann, J. & Sures, R. (2003). Effectiveness of information systems security in IT organizations in Malaysia. Communications, APCC 2003. ***In: The 9th Asia-Pacific Conference on,*** 2. IEEE.

Bahtiyar, S. & aglayan, M.U. (2013). Trust assessment of security for e-health systems. ***Electronic Commerce Research and Applications***, 13(3), 164–177.

Beas, M.I. & Salanova, M. (2006). Self-efficacy beliefs, computer training and psychological well-being among information and communication technology workers. ***Computers in Human Behavior***, 22, 1043–1058.

Brady, J.W. (2010). ***An investigation of factors that affect HIPAA security compliance in academic medical centers***. Unpublished 3411810, Florida: Nova Southeastern University.

Brady, J.W. (2011). Securing health care: assessing factors that affect hipaa security compliance in academic medical centers. ***Paper presented at the System Sciences (HICSS), 44th Hawaii International Conference***, Hawaii, 4–7 January.

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, 523–548.

Celep, C. & Yilmazturk, O.E. (2012). The relationship among organizational trust, multidimensional organizational commitment and perceived organizational support in educational organizations. Procedia – Social and Behavioral Sciences, 46, 5763–5776.

Chan, M., Woon, I. & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. ***Journal of Information Privacy and Security***, 1(3): 18–41.

Chang, A.J.; Wu, C.Y. & Liu, H.W. (2012). The effects of job satisfaction and organization commitment on information security policy adoption and compliance. ***Paper presented at the Management of Innovation and Technology (ICMIT), IEEE International Conference on***, 11–13 June.

Da Veiga, A. & Eloff, JHP. (2010). A framework and assessment instrument for information security culture. ***Computers and Security,*** 29: 196–207.

Da Veiga, A. & Martins, N. (2015). Improving the information security culture through monitoring and implementations actions illustrated through a case study. ***Computers & Security,*** 49, 162–176.

Guo, Kh. (2013). Security-related behavior in using information systems in the workplace: a review and synthesis. ***Computers & Security***, 32: 242–251.

Hair, J.F., Black, W.C., Babin, B.J. (2010). ***Multivariate Data Analysis: A Global Perspective.*** Upper Saddle River: Pearson Prentice Hall.

Herath, T. & Rao, H.R. (2009). Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. ***Decision Support Systems,*** 47, 154–165.

Hogler, R., Henle, C. & Gross, M. (2013). Ethical behavior and regional environments: the effects of culture, values, and trust. ***Employee Responsibilities and Rights Journal***, 25: 109–121.

Hu, Q., Dinev, T., Hart, P. & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture. ***Decision Sciences***, 43(4): 615–659.

Huang, D-L., Rau, P.L.P., Salvendy, G., Gao, F. & Zhoua, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. ***International Journal of Human-Computer Studies***, 69: 870–883.

Huang, E. and Chuang, M.H. (2007). Extending the theory of planned behavior as a model to explain post-merger employee behavior of IS use. ***Computers in Human Behavior,*** 23: 240–257.

Ifinedo, P. (2012). Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. ***Computers and Security***, 31: 83–95.

Johnston, A.C. & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. ***Information Management and Computer Security,*** 16: 5–19.

Kankanhalli, A., Teo, H-H., Tan, B.C.Y. & Wei, K.K. (2003). An integrative study of information systems security effectiveness***. International Journal of Information Management,*** 23(2), 139–154.

Kim, C., Tao, W., Shin, N., Kim, K.S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. ***Electronic Commerce Research and Applications,*** 9(1), 84–95.

Knapp, K.J., Franklin, Morris, R. Jr. Marshall, T.E. (2009). Information security policy: an organizational-level process model. ***Computers & Security,*** 28(7): 493–508.

Koskosas, I., Kakulidis, K. & Siomos, C. (2011). Examining the linkage between information security and end-user trust. ***International Journal of Computer Science and Information Security,*** 9: 21–31.

Liao, C., Chen, J.L. and Yen, D.C. (2007). Theory of planning behavior (TPB) and customer satisfaction in the continued use of eservice: an integrated model. ***Computers in Human Behavior,*** 23: 2804–2822.

Lippert, S.K. and Davis, M. (2006) A conceptual model integrating trust into planned change activities to enhance technology adoption behavior. ***Journal of Information Sciences,*** 32: 434–448.

Madhavan, P. & Phillips, R.R. (2010). Effects of computer selfefficacy and system reliability on user interaction with decision support systems. ***Computers in Human Behavior,*** 26: 199–204.

Mcdermott, A.M., Conway, E., Rousseau, D.M. (2013). Promoting effective psychological contracts through leadership: the missing link between HR strategy and performance. ***Human Resource Management***, 52: 289–310.

Meillier, L.K., Lund, A.B. & Kok, G. (1997). Cues to action in the process of changing lifestyle. ***Patient Education and Counseling***, 30: 37–51.

Narayana, S. G., Ahmad, R. & Ismail, Z. (2010). Security threats categories in healthcare information systems. ***Health Information Journal***, 16, 201–209.

Ng, B-Y., Atreyi, K. & Yunjie, X. (2009). Studying users' computer security behavior: a health belief perspective. ***Decision Support Systems***, 46, 815–825.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. ***Computers and Security,*** 31: 673–680.

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. System sciences, HICSS 2007. ***In: 40th Annual Hawaii International Conference on.*** IEEE.

Parsons, K., Mccormac, A., Butavicius, M. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). ***Computers and Security,*** 42, 165–176.

Puhakainen, P. & Ahonen, R. (2006). ***Design theory for information security awareness.***

Rhee, H.S., Kim, C. and Ryu, Y.U. (2009). Self-efficacy in information security: its influence on end users' information security practice behavior. ***Computers and Security,*** 28(8), 816–826.

Rhee, Y.K. (2010). Different effects of workers' trust on work stress, perceived stress, stress reaction, and job satisfaction between Korean and Japanese workers. ***Safety and Health at Work***, 1: 87–97.

Safa, N.S., Von Solms, R. & Furnell, S. (2016). Information security policy compliance behaviour model in organizations. ***Computers & Security,*** 56: 70–82.

Shahnawaz, M.G. & Goswami, K. (2011). Effect of psychological contract violation on organizational commitment, trust and turnover intention in private and public sector Indian organizations. Vision (09722629) 15: 209–217.

Siponen, M., Mahmood, M.A. & Pahnila, S. (2014). Employees' adherence to information security policies: an exploratory field study. ***Information and Management,*** 51: 217–224.

Six, F. & Sorge, A. (2008). Creating a high-trust organization: an exploration into organizational policies that stimulate interpersonal trust building. ***Journal of Management Studies***, 45: 857–884.

Symantec, S. (2013). ***Internet Security Threat Report 2013*** (Vol. 18).

Tan, H.H. and Lim, A.K.H (2009) Trust in coworkers and trust in organizations. ***Journal of Psychology***, 143: 45–66.

Taylor, S. & Todd, P. (1995). Decomposition and crossover effects in the theory of planned behavior: a study of consumer adoption intentions. ***International Journal of Research in Marketing***, 12: 137–155.

Torkzadeh, G. & Van Dyke. T.P. (2002). Effects of training on Internet self-efficacy and computer user attitudes. ***Computers in Human Behavior***, 18: 479–494.

Uffen, J. & Breitner, M.H. (2013). Management of technical security measures: an empirical examination of personality traits and behavioral intentions. System Sciences (HICSS), ***2013 46th Hawaii International Conference on.*** IEEE.

Utami, A.F., Bangun, Y.R. & Lantu, D.C. (2014). Understanding the role of emotional intelligence and trust to the relationship between organizational politics and organizational commitment. ***Procedia – Social and Behavioral Sciences,*** 115: 378–386.

Van Deursen, N., Buchanan, W.J. & Duff, A. (2013). Monitoring information security risks within health care. ***Computers & Security,*** 37: 31–45.

Williams, P.A.H. (2008). In a 'trusting' environment, everyone is responsible for information security. ***Information Security Technical Report,*** 13, 207–215.

Williams, PAH. (2009). Capturing culture in medical information security research. ***Methodological Innovations Online***, 4: 15–26.

Wood, C.C. & Banks, WW. Jr. (1993). Human error: an overlooked but significant information security problem. ***Computers and Security,*** 12(1): 51–60.

Woodhouse, S. (2007). Information security: end user behavior and corporate culture. Computer and Information Technology. CIT 2007. ***In: 7th IEEE International Conference on***. IEEE.

Workman, M., Bommer, W.H. & Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. ***Computers in Human Behavior,*** 24: 2799–2816.