DOI: http://dx.doi.org/10.22059/jitm.2016.57229

مدیریت فناوری اطلاعات
Journal of Information Technology Management

دانشکدهٔ مدیریت دانشگاه تهران
دورهٔ ۸، شمارهٔ ۲
تابستان ۱۳۹۵
ص. ۲۳۰- ۲۱۵

شناسایی الگوهای ذهنی کارمندان در خصوص سیاست‌های امنیت اطلاعات

ریحانه زهرا اسفندیارپور[۱]، مرتضی اکبری[۲]

چکیده: امنیت سیستم‌های اطلاعاتی، یکی از مهم‌ترین چالش‌های سازمان‌های امروزی است. بیشتر سازمان‌ها از فناوری‌های امنیتی استفاده می‌کنند، اما به این نتیجه رسیده‌اند که فناوری به تنهایی کافی نیست و تهدید اصلی برای امنیت سازمان از کارمندانی نشئت می‌گیرد که با سیاست‌های امنیت سازمان موافق نیستند. بنابراین حوزهٔ رفتارهای امنیتی کاربران نهایی در سازمان، توجه جدی سازمان‌ها را به خود جلب کرده است. مطالعات اخیر نشان داده است که کاربران نهایی، دیدگاه‌های امنیتی متفاوتی دارند که موجب ناتوانی در نظارت بر رفتارهای امنیتی کاربران شده است. این پژوهش با بهره‌مندی از روش کیو، تلاش می‌کند الگوهای ذهنی کارمندان در خصوص سیاست‌های امنیت اطلاعات را در راستای همراه‌کردن کارمندان با الزامات امنیتی سازمان، شناسایی کند. بدین منظور، پس از بررسی مطالعات پیشین، ارزیابی و جمع‌بندی فضای گفتمان، عبارات کیو انتخاب شدند و ۳۱ نفر از کارمندان شرکت پخش فراورده‌های نفتی آنها را رتبه‌بندی کردند؛ سپس عبارات تحلیل و چهار الگوی ذهنی شناسایی و بدین ترتیب دسته‌بندی شدند: ارزیابان، متعهدان، منسوبان و افرادی که ابزارهای بازدارندگی را در جهت همراهی با سیاست‌های امنیت اطلاعات مفید می‌دانند.

واژه‌های کلیدی: الگوهای ذهنی، پذیرش سیاست‌های امنیت اطلاعات، روش‌شناسی کیو، شرکت پخش فرآورده‌های نفتی.

۱. دانشجوی دکتری مدیریت سیستم‌ها، پردیس فارابی دانشگاه تهران، قم، ایران
۲. استادیار گروه کارآفرینی فناورانه، دانشکدهٔ کارآفرینی دانشگاه تهران، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹٤/۰٦/۰٦
تاریخ پذیرش نهایی مقاله: ۱۳۹۵/۰۲/۰۳
نویسندهٔ مسئول مقاله: ریحانه زهرا اسفندیارپور
E-mail: esfandiarpour@ut.ac.ir

مقدمه

سازمان‌های امروزی برای ادامهٔ حیات به سیستم‌های اطلاعاتی (IS)[1] متکی هستند (بولگرکو، کاوسگلو و بنباست، ۲۰۰۹ و ایفیندو، ۲۰۱۲)؛ زیرا سیستم‌های اطلاعاتی منابع داده‌ای با ارزش سازمانی را نگهداری می‌کنند. برای حفاظت از دارایی‌های حیاتی سیستم‌های اطلاعاتی در مقابل سوءاستفاده، استفادهٔ نادرست و تخریب، سازمان‌ها معمولاً از مجموعهٔ متنوع ابزارها و اقدامات، مانند فایروال‌ها، آنتی‌ویروس‌ها، سیستم‌های پشتیبان‌گیری، کنترل و محدودکردن دسترسی‌ها، کلیدهای رمزنگاری، سیستم‌های نظارت جامع و... استفاده می‌کنند. اگرچه این ابزارها و اقدامات، راه‌حل‌های فنی و فناورانه‌ای برای رفع مشکل به‌شمار می‌روند، اغلب برای حفاظت جامع از سیستم‌های اطلاعاتی کافی نیستند (ایفیندو، ۲۰۱۲ و ایفیندو، ۲۰۱۴).

پژوهشگرانی مانند وروم و ون سلمس (۲۰۰۴)، استانتون و همکاران (۲۰۰۵) و پهنیلا، سیپونن و محمود (۲۰۰۷) معتقدند سازمان‌هایی که به اندازهٔ ابزارهای فنی به ابزارهای غیرفنی در حمایت از دارایی‌ها و منابع سیستم‌های اطلاعاتی توجه کرده‌اند، در کوشش‌هایشان برای حفاظت از آنها موفق‌تر بوده‌اند (ایفیندو، ۲۰۱۲)، بنابراین سازمان‌ها باید بر چندین دیدگاه و چشم‌انداز برای حفاظت از دارایی‌ها و منابع اطلاعاتی تمرکز کنند. به‌علاوه، برخی از پژوهشگران ثابت کرده‌اند الزامات سازمانی ـ اجتماعی در محافظت از سیستم‌های اطلاعاتی اهمیت شایان توجهی دارند. در واقع یکی از دلایل ادامهٔ حوادث امنیتی سیستم‌های اطلاعاتی، سوءاستفاده‌ها و تخریب برای ضربه‌زدن به سازمان‌ها، این است که کارمندان ضعیف‌ترین حلقهٔ ارتباطی در تأمین امنیت سیستم‌های اطلاعاتی هستند و برای سازمان تهدید داخلی به‌شمار می‌روند؛ پس نگرش مفید برای حفاظت از منابع IS این است که سازمان‌ها باید بر ذهنیت کارمندان و رفتارهای آنها تمرکز کنند (ایفیندو، ۲۰۱۴؛ وانکه، سیپونن و پهنیلا، ۲۰۱۲ و استانتون و همکاران، ۲۰۰۵).

سازوکاری که سازمان‌ها برای شکل‌دهی یا تأثیر بر رفتارهای کارمندانشان به‌کار می‌برند، استفاده از قوانین، رهنمودها و دستورالعمل‌هایی با عنوان سیاست امنیت سیستم‌های اطلاعاتی (ISSP)[2] است. ادبیات نشان داده است در سازمان‌هایی که ISSP نتوانسته به امن نگه‌داشتن سازمان در مقابل سوءاستفاده، استفادهٔ نادرست و تخریب اطلاعات کمک کند، کارمندانش اغلب تمایلی به پذیرش چنین مستنداتی نداشته‌اند (ایفیندو، ۲۰۱۲). بسیاری از مطالعاتی که در سال‌های اخیر در حوزهٔ تطابق و پذیرش کارمندان سازمان با سیاست‌های امنیت اطلاعات صورت گرفته است، برمبنای تئوری‌های روان‌شناختی از جمله تئوری‌های رفتار برنامه‌ریزی‌شده، اقدام

1. Information Systems (IS)
2. Information System Security Policy (ISSP)

مستدل، انگیزش درونی و بیرونی، انگیزش حفاظت‌شده، اتصال اجتماعی و... و عوامل تأثیرگذار بر پذیرش سیاست‌ها بوده است.

برای هر سازمان ضروری است که بداند چگونه تفاوت‌های فردی بر پذیرش سیاست‌های امنیت اطلاعات تأثیر می‌گذارد و الزامات تطبیق رفتار فردی با این سیاست‌ها چیست. همچنین سازمان‌ها باید بدانند واکنش کارکنان در خصوص پیاده‌سازی امنیت اطلاعات در سازمان چیست و سرمایه‌گذاری‌های کلان آنها توانسته است بیشترین اثربخشی را در پاسخ به تهدیدهای داخلی و خارجی داشته باشد.

روش‌شناسی کیو فنی است که به پژوهشگر امکان می‌دهد ادراک و عقاید فردی را شناسایی و طبقه‌بندی کند و سپس بر اساس ادراک آنها به دسته‌بندی افراد بپردازد (خوشگویان‌فرد، ۱۳۸۶). حملهٔ سایبری به وزارت نفت در اردیبهشت ۱۳۹۱، آسیب‌ها و هزینه‌های فراوانی را به شرکت‌های تابعهٔ این وزارت از جمله شرکت پخش فراورده‌های نفتی تحمیل کرد. از آن زمان تاکنون، شرکت پخش فراورده‌های نفتی به‌منظور پیاده‌سازی سیستم مدیریت امنیت اطلاعات و خرید تجهیزات امنیتی، هزینه‌های گزافی می‌پردازد که اگر به عامل انسانی و همراهی کارمندان با سیاست‌های امنیت سازمان توجهی نکند، علاوه‌بر هدر رفتن تمام سرمایه‌گذاری‌ها، خسارت جبران‌ناپذیری به بار می‌آورد. از این رو، پژوهش حاضر در پی شناسایی الگوهای ذهنی کارمندان در خصوص سیاست‌های امنیت اطلاعات در شرکت پخش فراورده‌های نفتی و کمک به مدیران و مسئولان فناوری اطلاعات برای توجه به مسائل انسانی و تفکرات و همراهی کارکنان با مسائل امنیتی است.

پیشینهٔ نظری پژوهش

پژوهش‌های گسترده‌ای در زمینهٔ عوامل تأثیرگذار بر پذیرش سیاست‌های امنیت اطلاعات در سازمان‌ها صورت پذیرفته است که با هدف ارائهٔ مدلی بر مبنای تئوری‌های اجتماعی ـ شناختی، بازدارندگی و... اجرا شده‌اند؛ اما تاکنون مطالعه‌ای که بر دیدگاه و نگرش کارمندان در خصوص سیاست‌های امنیت اطلاعات تمرکز کند، انجام نشده است. در ادامهٔ مطلب به خلاصه‌ای از پژوهش‌های اجرا شده پرداخته می‌شود.

سیاست امنیت اطلاعات (ISP)

اقدام امنیتی مشترکی که بسیار در کانون توجه قرار دارد، تدوین و تنظیم سیاست امنیت اطلاعات است. سیاست امنیت اطلاعات، مجموعه‌ای از سیاست‌هاست که اهداف، اصول، قوانین و رهنمودهایی را دربردارد که مدیریت انتظار دارد کارکنان به آنها پای‌بند باشند و باید شامل شرح

مواردی چون پیامد نقض امنیت اطلاعات، استفاده در چارچوب مقررات از منابع کامپیوتری، مسئولیت‌های امنیت اطلاعات و آموزش کارمندان باشد (سمستاد، هالبرگ، لندهولم و بنگتسون، ۲۰۱۳). ویتمن (۲۰۰۴) بیان می‌کند که سیاست امنیت اطلاعات مطمئن، دستورالعمل مدیریتی برای روش انجام کار، هدایت و رویه‌های مناسب را که محتاطانه، مناسب و به نفع سازمان باشد، فراهم می‌کند. سیاست امنیت اطلاعات، کارمندان را در خصوص چگونگی استفاده از اطلاعات و فناوری اطلاعات در سازمان راهنمایی می‌کند. بسیاری از مطالعات گذشته که در زمینهٔ امنیت سیستم‌های اطلاعاتی انجام شده‌اند، تأکید کرده‌اند که اثربخشی امنیت سیستم‌های اطلاعاتی با مسائل فنی مرتبط است، در صورتی که باید بر هر دو معیارهای فنی و غیرفنی توجه شود؛ به این معنا که پای‌بندی به سیاست‌های امنیت اطلاعات سازمان، شامل پذیرش اقدامات مرتبط با فناوری اطلاعات و موافقت با معیارهای غیرفنی است. از جمله اقدامات مرتبط با فناوری اطلاعات، استقرار نرم‌افزار آنتی‌ویروس، فایروال‌ها، سیستم‌های تشخیص نفوذ است؛ در حالیکه موافقت با مباحث غیرفنی شامل مسائلی چون پذیرش قوانین، رویه‌ها و الزامات امنیت اطلاعات می‌شود (اسپورلینگ، ۱۹۹۵، چنگ، وو و لیو، ۲۰۱۲).

بررسی ادبیات نشان داده است تهدید اصلی امنیت سیستم‌های اطلاعاتی از جانب کارمندانی است که با سیاست‌ها و رویه‌های امنیت سیستم‌های اطلاعاتی موافق یا سازگار نیستند. برای اطمینان از پذیرش سیاست‌های امنیت اطلاعات توسط کارمندان، روش‌های متفاوتی ارائه شده است.

پیشینهٔ تجربی پژوهش

مطالعات در خصوص پیروی از سیاست‌های امنیت اطلاعات به سه دستهٔ زیر تقسیم می‌شود:

مطالعات مفهومی

این مطالعات، رهنمودها و راهکارهایی را دربردارد که برای بهبود تطابق کارکنان با سیاست‌های امنیت اطلاعات، امکان کنش متقابل در برابر مشکلات پیش‌آمده را می‌دهد. در این مطالعات از تئوری‌ها استفاده نمی‌شود و شواهد تجربی برای حمایت از اصول و پیشنهادها ارائه نمی‌دهد؛ بلکه دربرگیرندهٔ برنامه‌های آگاهی‌دهنده و استفاده از نرم‌افزارهایی به‌منظور تطابق کارمندان با سیاست‌های امنیت است. برای مثال فرنل (۲۰۰۲ و ۲۰۰۵) با اشاره به لزوم آگاهی امنیتی، به توصیف کاربرد نرم‌افزاری می‌پردازد که افراد را به آموزش امنیتی خودگام ترغیب می‌کند. نرم‌افزار، محیط کاربرپسندی را برای شبیه‌سازی و مطالعهٔ چند سناریو از پیش تعریف‌شده فراهم می‌کند. همچنین وی معتقد است اعمال ویژگی‌های امنیتی در نرم‌افزارها که یافتن، درک و

استفاده از آنها برای کاربر آسان باشد، در محافظت از دارایی‌های امنیتی تأثیرگذار است (فرنل، گنناتو و دولند، ۲۰۰۲ و فرنل، ۲۰۰۵). وود (۱۹۹۵) ۵۳ راهنمایی را برای اطمینان از تطابق کارمندان با رویه‌های امنیت سیستم‌های اطلاعاتی تهیه کرده است. اسپورلینگ (۱۹۹۵) بیان می‌کند که ارتقای برنامه‌های امنیتی باید بخشی از فرهنگ، فلسفه و چشم‌انداز سازمان باشد استانتون و همکاران (۲۰۰۵) و کاتسیکاس (۲۰۰۰) روشی را برای تعیین نیازهای آموزشی کارکنان در ارتباط با امنیت سیستم‌های اطلاعاتی پیشنهاد داده است (پهنیلا و همکاران، ۲۰۰۷).

مطالعات با مدل‌های نظری بدون شواهد تجربی

این دست از مطالعات، بینش مبتنی بر تئوری را برای راه‌های افزایش تطابق کارمندان با سیاست‌های امنیت سیستم‌های اطلاعاتی، فراهم می‌کنند؛ اما هیچ‌گونه شواهد تجربی برای حمایت از این بینش ارائه نمی‌دهند. این مدل‌ها پیشنهاد می‌کنند که هر دو راه‌حل اجتماعی و تکنیکی می‌تواند برای کاهش سوءاستفادهٔ کامپیوتری استفاده شوند (سیپونن، محمود و پهنیلا، ۲۰۱۴). این مطالعات مدل ایتیس و کونلی را که با هدف بررسی علت درگیری کارکنان در رفتارهای نقض سیاست‌های امنیت اطلاعات ارائه شده است، بسط داده‌اند (آیتس و کونولی، ۲۰۰۳). مدل مفهومی سیپونن (۲۰۰۰) برای آگاهی سیستم‌های اطلاعاتی/ امنیت سازمانی که به ماهیت هنجاری و تجویزی رهنمودهای کاربران توجه می‌کند و به منظور درک رفتار کاربران به‌کار می‌رود، شامل تئوری رفتار برنامه‌ریزی‌شده، انگیزش درونی و مدل پذیرش فناوری است (سیپونن،۲۰۰۰).

جانگ، وو و لیو (۲۰۱۲) تأثیر رضایت شغلی، تعهد سازمانی و طرز تفکر بر نیت پذیرش سیاست امنیت اطلاعات را با استفاده از تئوری‌های رفتار برنامه‌ریزی‌شده، انگیزش حمایت‌شده و تئوری اقدام مستدل توضیح می‌دهد. لی و همکارش مدلی را با استفاده از تئوری جرم‌شناسانه، اتصال اجتماعی، یادگیری اجتماعی برای توصیف سوءاستفادهٔ کامپیوتری گسترش داده‌اند (لی و لی، ۲۰۰۲).

مطالعات تجربی مبتنی بر تئوری‌ها

این دست از مطالعات، مطالعاتی مبتنی بر تئوری هستند که به‌طور تجربی آزمون شده‌اند و اعتبار آنها به تأیید رسیده است. در جدول ۱ خلاصه‌ای از این مطالعات و تئوری‌های استفاده شده در آنها درج شده است.

جدول ۱. خلاصه‌ای از مطالعات تجربی مبتنی بر تئوری‌ها

محققان	تئوری‌های استفاده‌شده	جامعهٔ آماری	هدف مقاله
بولگرکو، کاوسگلو و بنباست، ۲۰۱۰	تئوری رفتار برنامه‌ریزی‌شده	استفاده از پرسشنامهٔ الکترونیکی برای نظرخواهی از ۴۶۴ کارمند	به بررسی تأثیر اعتقاد کارکنان به پیامدهای تطابق یا عدم تطابق با سیاست‌های امنیت اطلاعات، هنجارهای ذهنی و خودباروری و همچنین تأثیر آگاهی امنیتی می‌پردازد.
بولگرکو و همکاران، ۲۰۰۹	تئوری رفتار برنامه‌ریزی‌شده	۴۶۴ شرکت‌کننده	به بررسی تأثیر دو عامل آگاهی امنیت اطلاعات و درک مناسب از الزامات سیاست امنیت اطلاعات پرداخته است.
چنگ، لی، هولمک و ژای، ۲۰۱۳	تئوری بازدارندگی عمومی، تئوری اتصال اجتماعی	۱۸۵ کارمند	عوامل کنترل رسمی و غیررسمی برمبنای مدل نظری از تئوری بازدارندگی و اتصال اجتماعی برای درک رفتار کارمندان بررسی شده است.
وانکه و همکاران، ۲۰۱۲	تئوری عادت و انگیزش حفاظت‌شده	۲۱۰ مدیر فناوری اطلاعات	در این مقاله از مدل یکپارچه‌شدهٔ تئوری عادت و انگیزش حفاظت‌شده برای بررسی پذیرش سیاست‌های امنیت اطلاعات استفاده شده است.
سیپونن و همکاران، ۲۰۱۴	تئوری‌های اقدام مستدل، انگیزش حفاظت‌شده و ارزیابی شناختی	۶۶۹ کارمند از ۴ شرکت فنلاند	با استفاده از مدلی مبتنی بر چند نظریه، به بررسی تأثیر شدت تهدیدهای درک‌شده، آسیب‌پذیری درک‌شده، اعتقادهای هنجاری، پاداش‌ها، خودباوری و اثربخشی پاسخ بر نیت پذیرش سیاست‌های امنیت اطلاعات پرداخته است.
تجاسوینی و رائو، ۲۰۰۹	پارادایم عامل	۳۱۲ کارمند از ۷۷ سازمان	تأثیر انگیزش درونی، بیرونی و مجازات‌ها را بر نیت پذیرش سیاست امنیت مورد بررسی قرار داده است.
ایفیندو، ۲۰۱۲	تئوری‌های رفتار برنامه‌ریزی‌شده و انگیزش حفاظت‌شده	۱۲۴ مدیر کسب‌وکار و متخصصان سیستم‌های اطلاعاتی	به‌کمک مدل یکپارچه‌ای از تئوری‌های رفتار برنامه‌ریزی‌شده و انگیزش حفاظت‌شده، به بررسی تأثیر خودباوری، هنجارهای ذهنی، اثربخشی پاسخ، درک آسیب‌پذیری، طرز تفکر در خصوص پاداش تطابق و هزینهٔ پاسخ پرداخته است.
ایفیندو، ۲۰۱۴	تئوری‌های اتصال اجتماعی، رفتار برنامه‌ریزی‌شده و شناخت اجتماعی[1]	۷۶۰۰ پرسشنامهٔ الکترونیکی مدیر کسب‌وکار و متخصصان سیستم‌های اطلاعاتی	این مطالعه پذیرش سیاست‌های امنیت اطلاعات از دیدگاه‌های نظری پیوند اجتماعی، نفوذ اجتماعی و پردازش شناختی را بررسی کرده است.

1. Social cognitive theory

ادامهٔ جدول ۱

محققان	تئوری‌های استفاده‌شده	جامعهٔ آماری	هدف مقاله
سان، ۲۰۱۱	تئوری بازدارندگی عمومی	۶۰۲ کارمند ایالت متحدهٔ آمریکا	تأثیر انگیزش درونی و بیرونی بر پذیرش سیاست‌های امنیت اطلاعات را بررسی قرار کرده است.
تجاسوینی و رائو، ۲۰۰۹	تئوری‌های رفتار برنامه‌ریزی‌شده، انگیزش حفاظت‌شده و بازدارندگی	۳۱۲ کارمند در ۷۸ سازمان	با استفاده از تئوری‌های انگیزش حفاظت‌شده، بازدارندگی و نقش تعهد و با این فرض که پذیرش اقدامات امنیت اطلاعات تحت تأثیر عوامل محیطی، رفتاری و سازمانی قرار می‌گیرد، مدل یکپارچه‌ای تحت لوای تئوری رفتار برنامه‌ریزی‌شدهٔ تیلور و تاد توسعه داده است.
سیپونن و همکاران، ۲۰۰۶	تئوری انگیزش حفاظت‌شده	۹۱۹ کارمند از ۵ شرکت	تئوری انگیزش حفاظت‌شده با عواملی از جمله وضوح[1] و اعتقادهای هنجاری برای بررسی نیت پذیرش سیاست‌های امنیت اطلاعات بسط داده شده است.
پهنیلا و همکاران، ۲۰۰۷	تئوری‌های اقدام مستدل، انگیزش حفاظت‌شده و بازدارندگی	۲۴۵ کارمند	مدل نظری که شامل عوامل تأثیرگذار بر سیاست امنیت اطلاعات است را گسترش داده‌اند. همچنین تأثیر کیفیت اطلاعات، طرز تفکرها، اعتقادهای هنجاری، ارزیابی تهدید، شرایط تسهیل‌کننده، تحریم‌ها و پاداش‌ها را ارزیابی کرده‌اند.

روش کیو به‌منزلهٔ نوعی ابزار تحقیقاتی، در رشته‌های متنوعی از جمله پرستاری، پزشکی، دامپزشکی، بهداشت عمومی، حمل‌ونقل، آموزش‌وپرورش، جامعه‌شناسی، ارتباطات تلفن همراه و... به‌کار می‌رود. این روش به‌ویژه زمانی مفید است که محققان به‌دنبال کشف و توصیف ذهنیت‌های متفاوت افراد نسبت به موضوعی خاص‌اند (سایت ویکی پدیا انگلیسی)[2].

مطالعات بسیاری در حوزهٔ عوامل مؤثر بر پذیرش سیاست‌های امنیت اطلاعات وجود دارد؛ اما تاکنون مطالعه‌ای با محوریت شناسایی الگوهای ذهنی کارمندان و تفکرات آنها در این خصوص صورت نگرفته است. برای مدیران مهم است که از درک کارمندان سازمان نسبت به سیاست‌های اعمال‌شده آگاه شوند. این مقاله تلاش می‌کند با استفاده از روش کیو نسبت به شناسایی این تفکرات اقدام نماید.

1. Visibility
2. https://en.wikipedia.org/wiki/Q_methodology

روش‌شناسی پژوهش

برای شناسایی ذهنیت کارمندان شرکت پخش فراورده‌های نفتی در خصوص سیاست‌های امنیت اطلاعات، از روش‌شناسی کیو استفاده شد. روش‌شناسی کیو با پذیرش اینکه انسان‌ها بر اساس تصاویری که از واقعیت دارند، عمل می‌کنند ـ نه براساس خود واقعیت ـ سازه‌گرایی معرفت‌شناسانه را انتخاب می‌کند. معمولاً روش‌شناسی کیو را پیوند بین روش‌های کیفی و کمّی می‌دانند؛ زیرا از یک‌سو، افراد نمونه به‌طور هدفمند و به تعداد کم انتخاب می‌شوند که آن را به روش کیفی نزدیک می‌کند و از سوی دیگر، یافته‌ها از طریق تحلیل عاملی، به‌صورت کاملاً کمی به‌دست می‌آیند (خوشگویان‌فرد، ۱۳۸۶).

روش کیو طی پنج گام اجرا می‌شود. در گام اول از طریق مطالعات کتابخانه‌ای، ادبیات تحقیق بررسی‌شده و پیش‌زمینهٔ گام‌های بعدی فراهم می‌آید. محقق با اجرای گام اول نسبت به موضوع، شناخت عمیقی کسب می‌کند. در گام دوم با برگزاری مصاحبه و بررسی اسناد و مدارک، در خصوص مسائل مرتبط با تحقیق اطلاعات تکمیلی به‌دست می‌آید. با توجه به اینکه در روش‌شناسی کیو نمونهٔ افراد از میان کسانی انتخاب می‌شود که ارتباط خاصی با موضوع تحقیق دارند (کور، ۲۰۰۱) در گام دوم این تحقیق با ۱۰ نفر از کارمندان شرکت پخش فراورده‌های نفتی که با سیستم‌های اطلاعاتی و اطلاعات محرمانه در ارتباط بودند و با سیاست‌های امنیت اطلاعات آشنایی داشتند، مصاحبه شد. در این پژوهش طبق اصول مطرح‌شده در روش کیو، مصاحبه‌ها با استفاده از تحلیل تم برگزار شد. در این‌گونه مصاحبه‌ها جمع‌آوری اطلاعات تا زمانی ادامه می‌یابد که داده‌های جدید جمع‌آوری‌شده با داده‌هایی که قبلاً جمع‌آوری شده‌اند، تفاوتی نداشته باشد. لینکلن و گوبا معتقدند در مطالعه‌ای که با دقت هدایت شود و انتخاب نمونه به‌صورت تکاملی و تعاقبی باشد، می‌توان با حدود ۱۰ شرکت‌کننده به مرز اشباع رسید (خوشگویان‌فرد، ۱۳۸۶). در این پژوهش، محقق پس از انجام اجرای ۱۰ مصاحبه به اشباع رسید. نتایج گام اول و دوم، فضای گفتمان را تشکیل می‌دهد. در گام سوم باید با ارزیابی و جمع‌بندی محتویات فضای گفتمان به آن سروسامان داد و نمونه‌ای از عبارات را به‌عنوان نمونهٔ کیو از میان آنها انتخاب کرد. مک‌کئون و توماس تعدادی بین ۳۰ تا ۱۰۰ عبارت را برای نمونهٔ کیو پیشنهاد کرده‌اند. دانر معتقد است تعداد مناسب عبارات برای آنکه یافته‌ها دارای اعتبار آماری باشند، بین ۲۰ تا ۶۰ عبارت است (کور، ۲۰۰۱). در این تحقیق به کمک سه صاحب‌نظر و متخصص در این زمینه، تعداد گزاره‌ها از ۶۳ گزاره به ۳۴ گویه تقلیل یافت و تلاش شد عباراتی که معنا و مفهوم متمایزی از سایر عبارات دارند، انتخاب شوند. در گام چهارم مشارکت‌کنندگان به مرتب‌سازی و دسته‌بندی کارت‌های دستهٔ کیو می‌پردازند. در واقع، گام چهارم مرحلهٔ گردآوری داده‌هاست. در

این مرحله مشارکت‌کنندگان به‌صورت هدفمند انتخاب شدند؛ یعنی افرادی از اهالی گفتمان که به دلایل شغلی، تجربی و غیره، ارتباط خاصی با موضوع داشتند. در پژوهش حاضر ۳۱ نفر از میان کارکنان شرکت پخش فراورده‌های نفتی شاغل در واحدهای مالی، فروش، اداری و فناوری اطلاعات انتخاب شدند و در اجرای مراحل مرتب‌سازی کیو مشارکت کردند (شکل ۱).

در گام آخر، به تحلیل داده‌های گردآوری‌شده با روش تحلیل عاملی کیو و تفسیر عامل‌های استخراج‌شده پرداخته می‌شود.

شایان ذکر است برای بررسی ضریب پایایی در این تحقیق، از پایایی آزمون ـ آزمون مجدد استفاده شد که نتیجهٔ آن ۸۵ درصد بود

بسمه تعالی

نیروی انسانی یکی از مهم‌ترین عوامل حفاظت و امنیت اطلاعات هر سازمان است. با عنایت به پیاده‌سازی سیستم مدیریت امنیت اطلاعات در شرکت پخش فراورده‌های نفتی و اجرای سیاست‌های امنیتی، از شما درخواست می‌شود بر اساس دستورالعمل زیر و اهمیت تأثیرگذاری هر یک از عبارت‌ها در پذیرش و همراهی کارمندان با سیاست‌های امنیت سازمان، آنها را اولویت‌بندی نمایید.

با تشکر

مشخصات :

جنس: زن: مرد: تحصیلات : واحد:

دستورالعمل مرتب‌سازی

۱. ابتدا تک‌تک جمله را مرور کنید؛

۲. جملات را به سه دسته تقسیم نمایید: دو دستهٔ ۱۴ تایی و یک دستهٔ ۶ تایی. ۱۴ دستهٔ اول جملاتی هستند که با آنها موافق‌اید؛ با جملات دستهٔ ۱۴ تایی دوم مخالف هستید و با ۶ جمهٔ آخر نه مخالف و نه موافق‌اید.

۳. اکنون ۱۴ جمله‌ای که با آن موافق‌اید را در نظر بگیرید؛ از میان آنها، دو جمله‌ای که با آن بیشتر موافق‌اید را در کادر +۴ قرار دهید. سپس از میان ۱۲ کادر باقی‌مانده، سه جمله‌ای که بیشتر با آنها موافق هستید را در کادر +۳ قرار دهید و به همین ترتیب چهار جمله را در +۲ و پنج جملهٔ آخر را در +۱ قرار دهید.

۴. در خصوص ۱۴ جمله‌ای که با آنها مخالف هستید نیز مانند دستورالعمل شمارهٔ ۳ اقدام فرمایید.

شکل ۱. نمونه‌ای از پرسشنامهٔ کیو

تجزیه‌وتحلیل نتایج

برای شناسایی الگوهای ذهنی، رتبه‌بندی و مرتب‌سازی کیو، داده‌های جمع‌آوری‌شده وارد نرم‌افزار SPSS شدند و تحلیل عاملی کیو با استفاده از این داده‌ها و تشکیل ماتریس همبستگی انجام شد. پس از استخراج عامل‌ها به روش مؤلفهٔ اصلی، با بهره‌مندی از روش واریماکس عامل‌ها هفت بار چرخش یافتند. بدین ترتیب چهار الگوی ذهنی انتخاب شد که در جدول ۲ نمایش داده شده است.

جدول ۲. عامل‌های شناسایی‌شده و امتیازهای عاملی عبارت‌ها

گزاره‌ها	امتیاز عاملی			
	الگوی ذهنی اول	الگوی ذهنی دوم	الگوی ذهنی سوم	الگوی ذهنی چهارم
۱. اعتقاد به کمک در امنیت اطلاعات سازمان با پیروی از سیاست‌های امنیتی	-۱	-۲	۳	۰
۲. اعتقاد به ارتقای عملکرد سازمان در صورت پیروی از سیاست‌های امنیتی	۰	-۱	۳	۱
۳. اعتقاد به ضرر و زیان سازمان در صورت پیروی‌نکردن از سیاست‌های امنیتی	۰	-۳	۲	۰
۴. اهمیت، علاقه‌مندی و با ارزش‌بودن شغل برای کارمند	۰	-۳	۴	۲
۵. علاقه و وفاداری نسبت به سازمان	-۱	۰	۴	۳
۶. تمایل به تلاش و صرف انرژی برای موفقیت سیاست‌های امنیت اطلاعات در سازمان	-۲	۰	۳	۲
۷. ارزش قائل‌شدن به شرکت در جلسه‌های امنیت اطلاعات	-۱	-۲	۲	-۱
۸. مشارکت فعالانه در فعالیت‌های رشد و ارتقای سازمان	۰	-۱	۲	۲
۹. اخطار و مجازات از طرف سازمان در صورت نقض قوانین امنیتی	-۳	-۴	-۱	۰
۱۰. اطمینان از مانیتورینگ نقص امنیت اطلاعات توسط واحد کامپیوتر	-۳	۳	۰	۴
۱۱. اطمینان از کشف و ثبت نقض قوانین و سیاست‌های امنیت اطلاعات	-۲	۱	-۱	۴
۱۲. احترام به دیدگاه‌ها و عقاید همکاران در خصوص سیاست‌های امنیت اطلاعات	-۳	۲	-۱	-۱
۱۳. اعتقاد به موافقت سایر کارمندان سازمان با سیاست‌های امنیت اطلاعات	-۲	۳	-۱	-۴
۱۴. انتظار مدیریت ارشد سازمان از کارمندان برای پیروی از سیاست‌های امنیت اطلاعات	۰	۴	۲	۱
۱۵. انتظار همکاران سازمان برای پیروی از سیاست‌های امنیت اطلاعات	-۲	-۲	-۲	-۲
۱۶. انتظار مستقیم رئیس از کارمند، برای پیروی از سیاست‌های امنیت اطلاعات	-۱	۴	۰	۱
۱۷. انتظار واحد کامپیوتر از کارمندان سازمان برای پیروی از سیاست‌های امنیت اطلاعات	-۴	-۱	-۴	-۲
۱۸. توانایی به‌کارگیری ابزارها و سیاست‌های امنیت اطلاعات	۱	۱	-۲	۰
۱۹. توانایی پیروی از سیاست‌های غیرمرتبط با حوزهٔ کاری	-۱	-۱	-۲	-۳
۲۰. تجربهٔ کار در خصوص به‌کارگیری ابزارها و سیاست‌های امنیت اطلاعات	۲	۰	-۴	۳
۲۱. تخصص و تجربهٔ افراد در خصوص مسائل کامپیوتری و مباحث امنیت اطلاعات	۱	۲	-۳	۳
۲۲. واضح‌بودن سیاست نوشته‌شده	۰	۰	۱	-۳
۲۳. در دسترس‌بودن سیاست‌های امنیت	۱	۲	۰	-۳
۲۴. آموزش سیاست‌های امنیت اطلاعات	۱	۳	-۱	-۲
۲۵. مزیت‌های بیشتر امنیت اطلاعات برای سازمان نسبت به هزینه‌های انجام‌شده	۲	۱	-۲	۰
۲۶. درک تأثیر مثبت به‌کارگیری ابزارهای امنیتی در کار کارمندان در مقایسه با به‌کارنبردن آنها	۴	-۲	-۳	۲

ادامهٔ جدول ۲

گزاره‌ها	امتیاز عاملی			
	الگوی ذهنی اول	الگوی ذهنی دوم	الگوی ذهنی سوم	الگوی ذهنی چهارم
۲۷. درک آسیب‌پذیری سازمان در صورت همراهی‌نکردن با سیاست‌های امنیتی	۴	-۴	۰	۱
۲۸. درک اهمیت ابزارها و سیاست‌های امنیتی در جلوگیری از حملهٔ هکرها برای دسترسی به اطلاعات مالی و کارکنان	۱	۱	۰	-۱
۲۹. تجربهٔ قبلی در خصوص مشکلات دسترسی غیرقانونی و هک اطلاعات سازمان	۲	۲	۱	-۱
۳۰. ایجاد مشکلات جدی برای کارمند و سازمان در صورت دسترسی غیرقانونی به اطلاعات کامپیوتر کارمندان سازمان	۳	-۱	۱	-۴
۳۱. به خطر افتادن داده‌ها و منابع سازمان در صورت بی‌توجهی به رهنمودهای امنیتی	۲	۰	۱	-۲
۳۲. دریافت پاداش از سازمان در صورت رعایت الزامات امنیتی	۳	۱	۰	۱
۳۳. درک جدیت تهدیدهای رودرروی سازمان	۳	۰	۱	۰
۳۴. عادت به رعایت الزامات امنیتی	-۴	-۳	-۳	-۱

در جدول‌های ۳ و ۴ بارهای عاملی استخراج‌شده به نمایش گذاشته شده‌اند. با توجه به الگوی ذهنی شناسایی‌شده (بارهای عاملی بزرگ‌تر از ۰/۷) در جدول‌های ۳ و ۴، مشخص می‌شود که اشخاص ۲، ۳، ۸، ۱۱ و ۲۵ به‌طور مشترک عامل الگوی ذهن اول، اشخاص ۱۰ و ۱۶ عامل الگوی ذهنی دوم، اشخاص ۴، ۲۲ و ۲۸ عامل الگوی ذهنی سوم و اشخاص ۲۴ و ۳۰ عامل الگوی ذهنی چهارم هستند. همچنین مقدار ویژهٔ هر عامل، سهمی از واریانس که توسط هر عامل تبیین می‌شود و جمع تراکمی آنها، در جدول ۵ نمایش داده شده است. همان‌گونه که دیده می‌شود جمع تراکمی واریانس کل تبیین‌شده توسط چهار عامل برابر ۶۵/۶۷ درصد از واریانس کل عوامل است.

جدول ۳. ماتریس عوامل شناسایی‌شده

عامل‌ها	۱	۲	۳	٤
۱	۰/۵۲۳	۰/۶۰۶	۰/۳۷۶	۰/۴۶۶
۲	۰/۷۹۰	-۰/۹۶	-۰/۴۷۰	-۰/۳۸۲
۳	۰/۳۰۳	-۰/۶۳۵	۰/۷۰۶	-۰/۰۸۳
۴	۰/۱۰۴	-۰/۴۶۹	-۰/۳۷۳	۰/۷۹۴

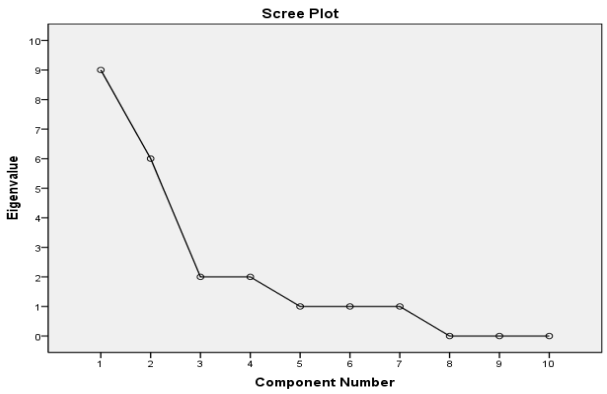
جدول ٤. ماتریس چرخش‌یافتهٔ عامل‌ها

	عامل‌ها			
	۱	۲	۳	٤
P2	۰/۹۴۷	۰/۰۲۹	۰/۱۳۶	−۰/۰۱۴
P11	۰/۹۱۸	۰/۰۳۵	−۰/۰۵۳	−۰/۱۴۳
P3	۰/۸۹۷	۰/۰۲۳	−۰/۰۳۹	−۰/۱۶۵
P8	۰/۷۵۷	۰/۲۸۷	−۰/۰۲۹	۰/۱۵۵
P25	۰/۷۴۳	۰/۰۲۸	−۰/۱۴۹	۰/۳۲۳
P16	۰/۰۲۵	۰/۸۰۴	−۰/۰۸۰	۰/۰۶۰
P10	۰/۰۹۱	۰/۷۱۰	۰/۱۵۳	۰/۳۲۱
P22	−۰/۱۶۵	۰/۰۶۰	۰/۷۸۲	۰/۴۵۷
P4	−۰/۰۸۱	−۰/۴۵۱	۰/۷۴۹	۰/۰۹۷
P28	−۰/۱۲۴	−۰/۰۷۲	۰/۷۳۱	۰/۴۰۵
P24	−۰/۰۶۲	۰/۱۷۴	۰/۱۷۸	۰/۸۸۲
P30	−۰/۰۸۲	۰/۱۸۸	۰/۱۷۰	۰/۸۶۵

جدول ۵. مقدار واریانس کل تبیین‌شده

عامل	کل	درصد از واریانس	تجمعی
۱	۹/۶۶۷	۳۱/۱۸۵	۳۱/۱۸۵
۲	۶/۰۵۵	۱۹/۵۳۱	۵۰/۷۱۶
۳	۲/۶۲۵	۸/۴۶۶	۵۹/۱۸۲
۴	۲/۰۱۳	۶/۴۹۳	۶۵/۶۷۵

در شکل ۲ نمودار سنگریزه نشان داده شده است. در این نمودار عامل‌ها با مقادیر ویژهٔ بیشتر از ۱ (کلانتری، ۱۳۸۲: ۳۰۷) که نشان‌دهندهٔ الگوهای ذهنی است، مشخص شده‌اند.



شکل ۲. نمودار سنگریزه

یافته‌های پژوهش

داده‌های پژوهش پس از تحلیل، چهار الگوی ذهنی را در خصوص پذیرش سیاست‌های امنیت اطلاعات در سازمان آشکار کرد و الگوهای حاصل بر اساس گزاره‌های متمایزکنندهٔ مهم، به‌ترتیب زیر نام‌گذاری و تحلیل شدند:

گروه اول ارزیابی‌کنندگان هستند. این گروه از کارمندان با ارزیابی شدت تهدیدها و آسیب‌پذیری سازمان در مقابل تهدیدهای امنیتی و مقایسهٔ هزینه و منفعت آن، به همراهی با سیاست‌های امنیت اطلاعات اقدام می‌کنند. این افراد با درک این موضوع که سازمان با تهدیدهای امنیتی جدی مواجه است و در صورت همراهی‌نکردن آنان، ضمن آسیب‌دیدن سازمان، مشکلات جدی برای کارمند و سازمان ایجاد می‌شود، با سیاست‌ها همراهی می‌کنند. دریافت پاداش مشوق آنان در این همراهی است (گزاره‌های ۲۷ ،۲۶، ۳۰، ۳۲ و ۳۳).

گروه دوم منسوبان یا افراد وابسته به هنجارهای ذهنی هستند. این افراد در صورت آگاهی از انتظارات مدیریت ارشد، مدیر مستقیم و همکاران، به‌منظور پیروی و رعایت الزامات امنیتی با سیاست‌ها همراهی می‌کنند (گزاره‌های ۱۲، ۱۳ و ۱۴).

گروه سوم افراد متعهد به سازمان هستند. این افراد نسبت به سازمان وفادارند و پیشرفت سازمان برای آنها مهم است، به همین دلیل خود را درگیر فعالیت‌هایی می‌کنند که سبب رشد و ارتقای سازمان می‌شود. این گروه معتقدند پیروی از سیاست‌های امنیت اطلاعات به ارتقای سازمان کمک می‌کند و برای شرکت در جلسه‌های امنیت اطلاعات ارزش قائل‌اند. با شناسایی این افراد در سازمان، می‌توان آنان را الگو قرار داد و از پتانسیلشان برای برقراری ارتباط با سایر کارکنان و توجیه‌کردن کارکنان بهره برد (گزاره‌های ۱، ۲، ۴، ۵، ۶، ۷ و ۸).

گروه چهارم افرادی هستند که ابزارهای بازدارندگی را برای همراهی با سیاست‌ها و الزامات امنیت اطلاعات مفید می‌دانند. این افراد در صورت اطمینان از نظارت بر نقض امنیت اطلاعات و کشف و ضبط آن توسط واحد کامپیوتر، سیاست‌های امنیت اطلاعات را رعایت می‌کنند. این افراد تخصص و تجربهٔ کامپیوتری را در این مورد مؤثر می‌دانند (گزاره‌های ۱۰، ۱۱ و ۲۱).

نتیجه‌گیری و پیشنهادها

پژوهش‌های متعددی در زمینهٔ عوامل مؤثر بر پذیرش سیاست‌های امنیت اطلاعات اجرا شده است که هدف آنها توسعهٔ مدلی تئوریکی بر پایهٔ تئوری‌های اجتماعی ـ روان‌شناختی بوده است. این پژوهش تلاش کرد برای اولین‌بار با بهره‌مندی از روش‌شناسی کیو، ذهنیت کارمندان را در خصوص سیاست‌های امنیت اطلاعات در سازمان شناسایی کند. این مطالعه طبقه‌بندی جدیدی

به ادبیات موجود افزود و تفکرات گوناگونی را در خصوص سیاست‌های امنیت اطلاعات بررسی کرد. پیش‌فرض مطالعهٔ حاضر بر این پایه بود که تصور کارمندان در خصوص سیاست‌های امنیت اطلاعات بر پذیرش و همراهی آنان با الزامات امنیتی، تأثیرگذار است. از این رو پس از مطالعهٔ منابع مختلف فضای گفتمان، نمونهٔ کیو انتخاب شد. با سپری‌شدن مرحلهٔ مرتب‌سازی نتایج، به تحلیل داده‌ها پرداخته شد و چهار الگوی ذهنی به‌دست آمد که این الگوها بر اساس گزاره‌های متمایزکننده‌ای که بیشترین امتیاز را داشتند، تحلیل شدند.

شناسایی این ذهنیت‌ها می‌تواند به‌عنوان مرجعی برای مدیران شرکت‌ها به‌منظور تعیین استراتژی مناسب در همراه‌کردن گروه‌های متفاوت کارکنان با سیاست‌های امنیت اطلاعات استفاده شود. ارزیابی‌کنندگان، افرادی هستند که با درک صحیح از آسیب‌پذیری سازمان و آگاهی از عواقب آن، با سیاست‌های سازمان همراهی می‌کنند. گروه منسوبان، نشان می‌دهد نفوذ اجتماعی در رفتارهای امنیتی می‌تواند نقش حیاتی ایفا کند؛ به‌طوری که اعتقادهای این گروه از کارکنان تحت تأثیر انتظارات مافوق و همکاران قرار می‌گیرد. متعهدان، افرادی هستند که به پیشرفت و ارتقای سازمان اهمیت می‌دهند و چنانچه درک کنند سیاست‌های امنیت اطلاعات به ارتقای سازمان می‌انجامد، با فعالیت‌های امنیتی سازمان همراه می‌شوند و در نهایت افرادی که ابزارهای بازدارندگی را مفید می‌دانند، در صورت اطمینان از کشف نقض سیاست‌های امنیت نسبت به رعایت مسائل امنیتی اقدام می‌کنند. در این میان گروه ارزیابی‌کنندگان بر سه الگوی دیگر غلبه می‌کند؛ زیرا کارمندان با ارزیابی و درک شدت آسیب‌پذیری سازمان در مقابل تهدیدهای امنیتی و ایجاد مشکلات جدی برای سازمان و کارمندان، در صورت نقض سیاست‌ها، به احتمال بیشتر با سیاست‌های امنیت سازمان همراهی خواهند کرد. بر اساس نتایج این پژوهش، کارمندان برخوردهای مختلفی نسبت به سیاست‌های امنیت اطلاعات دارند و این تفاوت‌ها برگرفته از تفاوت دیدگاه آنها نسبت به سیاست‌های امنیت اطلاعات است.

References

Aytes, K. & Connolly, T. (2003). A research model for investigating human behavior related to computer security. *Americas conference on information system (AMCIS)*. paper 260. Available in: http://aisel.aisnet.org/amcis2003/260.

Brown, S.R., Q (1996). Methodology and Qualitative research. *Qualitative Health Reseach*, 6(4): 561-567.

Bulgurcu, B., Cavusoglu, H. & Benbasat, L. (2009). Roles of Information Security Awareness and Perceived Fairness in Information Security Policy

Compliance, *Americas Conference on Information Systems,* AMCIS2009, San Francisco, California, Augus 6-9, 2009.

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

Chang, J., Wu, C. & Liu, H. (2012).The Effects of Job Satisfaction and Organization Commitment on Information Security Policy Adoption and Compliance. *Management of Innovation and Technology* (ICMIT). *IEEE International Conference on, Sanur Bali,* June 2012, DOI: 10.1109/ICMIT.2012.6225846.

Cheng, L., Li, Y., Li, W., Holmc, E. & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security,* 39: 447- 459.

Corr, S. (2001). An introduction to Q methodology, a Research Technique, British. *Journal of Occupational therapy*, 64(6): 293-297.

Furnell, S., Gennatou, M. & Dowland P. S. (2002). A prototype tool for IS security awareness and training. *International Journal of Logistics Information Management*, 15 (5): 352-357.

Furnell, S. M. (2005). Why users cannot use security. *Computers & Security*, 24(4): 274-279.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *computers & security*, 31 (1): 83-95.

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.

Kalantari, KH. (2003). *Data processing and analysis of socio-economic research*. Tehran: Sharif. (*in Persian*)

Katsikas, S. K. (2000). Health care management and information system security: awareness, training or education. *International Journal of Medical Informatics*, 60(2): 129-135.

Koshgoyanfard, A. (2007). *Q methodology*. Tehran: IRIB Research Center. (*in Persian*)

Lee, J. & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information management & computer security*, 10 (2): 57-63.

Pahnila, S., Siponen, M. & Mahmood, M. (2007). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*, DOI: 10.1109/HICSS.2007.206.

Siponen, M. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security*, 8(1): 31-41.

Siponen, M., Pahnila, S. & Mahmood, M. (2006). Factors Influencing Protection Motivation and IS Security Policy Compliance*, Innovations in Information Technology Conference*, Dubai, Nov 2006, DOI: 10.1109/INNOVATIONS. 2006.301907.

Siponen, M., Mahmood, A. & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2): 217–224.

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2013). Variables influencing information security policy compliance A systematic review of quantitative studies. *Information Management &Computer Security*, 22 (1): 42-75.

Son, J, (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48 (7): 296–302.

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security*, 3(2): 20-26.

Stanton, J.M., Stam, K.R., Mastrangelo, P.M. & Jolton, J.A. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2): 124-133.

Tejaswini, H. & Rao, R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems,* 47(2): 154–165.

Tejaswini, H. & Rao, R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2): 106–125.

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49(3-4): 190–198.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24(1): 43-57.