تاریخ دریافت:۹۵/۱۰/۱۰
تاریخ پذیرش نهایی:۹۶/۲/۲۳

فصلنامه دانش امنیتی
سال اول/شماره یکم/ بهار۱۳۹۶

بررسی عوامل انسانی موثر بر اثربخشی امنیت سامانه‌های اطلاعاتی

احمدعلی روح‌الهی[۱]
سیروس اقبال‌پور[۲]

چکیده

امنیت اطلاعات برای سازمان‌ها به مسئله‌ای حیاتی تبدیل شده است. امنیت سیستم‌های اطلاعاتی هر دو بُعد فناوری و افراد (عوامل انسانی) را دربرمی‌گیرد. پژوهش حاضر با هدف بررسی عوامل انسانی مؤثر بر اثربخشی امنیت سامانه‌های اطلاعاتی انجام شد. جامعه مورد مطالعه شامل همه کارشناسان و کاربران رایانه یکی از دانشگاه‌های نظامی در سطح شهر تهران بود. کارشناسان و کاربران رایانه این دانشگاه ۳۲۰ نفر بودند که ۱۷۵ نفر بر اساس جدول مورگان و به روش نمونه‌گیری تصادفی ساده انتخاب شدند. ابزار جمع‌آوری داده‌ها، پرسش‌نامه‌ای محقق‌ساخته بوده است. روایی و پایایی پرسش‌نامه احصاشده با استفاده از مدل‌سازی معادلات ساختاری و به وسیله نرم‌افزار لیزرل ۸/۵۴ مورد تأیید قرار گرفت. تحلیل داده‌های حاصل از مدل‌سازی معادلات ساختاری حاکی از آن است که شاخص‌های «فرهنگ امنیتی»، «آموزش امنیتی»، «مهارت امنیتی» و «تجربیات افراد» با اثربخشی امنیت سامانه‌های اطلاعاتی رابطه‌ای مثبت و معنادار دارد. در نتیجه با شناختی که از عوامل تأثیرگذار بر امنیت سامانه‌های اطلاعاتی حاصل می‌شود، می‌توان با ایجاد بهبود در این عوامل برای تشویق کاربران به استفاده از سامانه‌های اطلاعاتی گام برداشت.

واژگان کلیدی

امنیت اطلاعاتی، عوامل انسانی، فرهنگ امنیتی، آموزش امنیتی، مهارت‌های امنیتی و تجربیات افراد

---

۱ . عضو هیئت علمی دانشگاه هوایی شهید ستاری، دانشکده پرواز، گروه آموزشی مراقبت پرواز
۲ . دانشجوی کارشناسی ارشد مدیریت منابع انسانی، دانشگاه آزاد اسلامی واحد علوم تحقیقات

مقدمه

امروزه اطلاعات در سازمان‌ها و مؤسسات به منزله شاهرگ حیاتی محسوب می‌شود. دستیابی به اطلاعات و عرضه مناسب و سریع آن، همواره مورد توجه سازمان‌هایی بوده که اطلاعات در آنها، نقشی محوری و سرنوشت‌ساز داشته است (صنیعی، ۱۳۹۲: ۱۲۷). در حقیقت، حفاظت از اطلاعات و سیستم‌های اطلاعاتی سازمان یکی از ارکان مهم بقای آن محسوب می‌شود. بر این اساس، حفاظت از منابع اطلاعاتی سازمان (چه در مورد سیستم اطلاعاتی و چه اعضای سازمان) بسیار حیاتی و اجتناب‌ناپذیر است. بنابراین حمایت از اطلاعات و کاهش ریسک نسبت به قبل بسیار مهم‌تر و برجسته‌تر می‌شود (اسکو[1]، ۲۰۰۴: ۱۲۳). بررسی‌های انجام‌شده روی سازمان‌های مختلف نشان می‌دهد که تعداد زیادی از منابع اطلاعاتی سازمان‌ها در زمان‌های مختلف مورد حمله قرار گرفتند (بکچی و اودو،[2] ۲۰۰۴: ۶۸۴؛ امیتر و همکاران،[3] ۲۰۰۰: ۹۷؛ تیم پاسخگو به شرایط اضطراری،[4] ۲۰۰۴: ۲؛ گردون و همکاران،[5] ۲۰۰۴: ۱۱۸). حجم بالای اطلاعات در هر سازمان در قالب طرح‌ها، نقشه‌ها، سیاست‌ها، بخشنامه‌ها، مکاتبات، مستندات پروژه‌های پژوهشی و سایر اطلاعاتی که برای ذخیره‌سازی و پردازش در اختیار این فناوری قرار می‌دهیم، ما را بر آن می‌دارد تا به فکر حفاظت از آن نیز باشیم. به بیانی دیگر، اطلاعات مهم‌ترین دارایی و کلید رشد و موفقیت هر سازمان است. اگر مدیریت سازمان نتواند این دارایی مهم را از دسترس افراد غیرمجاز و سایر تهدیدها حفظ کند، به شدت آسیب می‌بینند.

ضرورت این پژوهش بدان علت بیشتر احساس می‌شود که در عصر حاضر سازمان‌ها با ارزش‌ترین دارایی خود را برای پردازش و ذخیره‌سازی در اختیار تجهیزات فناوری اطلاعات قرار می‌دهند. وابستگی به این فناوری باعث شده است که اگر در ارائه خدمات خللی پیش آید سازمان‌ها نتوانند به کار خود ادامه دهند. بدین ترتیب حیات سازمان‌ها ارتباطی نزدیک با سیستم‌های اطلاعاتی دارد. سیستم‌های اطلاعاتی نیز همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در ارائه خدمات هستند. از این رو سازمان‌ها برای ایمن ماندن از این آسیب‌ها باید به فکر امنیت اطلاعات باشند. از

1 . Schou
2 . Bagchi and Udo
3 . Ammeter, Douglas, Gardner, Hochwarter, Ferris
4 . Computer Emergency Response Team
5 . Gordon, L.A., et al.

آنجا که این‌گونه حوادث، مکرر، هزینه‌بر و از مهم‌تر تهدیدکننده امنیت اطلاعات هر سازمان هستند، مدیریت باید به صورت جدی به امنیت توجه کند تا بتواند از اطلاعات و سیستم‌های اطلاعاتی سازمانی حفظ و حمایت کند.

تا کنون بیشتر تحقیقاتی که در زمینهٔ امنیت سیستم‌های اطلاعاتی انجام شده، در زمینهٔ مسائل فنی و تکنیکی بوده است و در نتیجه نگرش به امنیت سیستم‌های اطلاعاتی به عنوان یک مسئلهٔ فنی بر تحقیقات امنیت سیستم‌های اطلاعاتی تسلّط داشته است (مگلاراس، ۲۰۰۲، ۶۲؛ کاتلین و کارلی، ۲۰۰۰: ۷۶؛ گری و آیسکت، ۲۰۰۳: ۴۳؛ جوز و آگاتا، ۲۰۰۲: ۴۸۲؛ ماریاتی و همکاران، ۲۰۰۵، ۴۷۲؛ گری، ۲۰۰۳: ۳۴). هایند[1] (۲۰۰۴) بیان می‌کند که در بیشتر تحقیقاتی که در زمینه امنیت سیستم‌های اطلاعاتی صورت گرفته است، یک نوع دید رویکرد فنی وجود داشته است و متخصصین امنیت اطلاعات بیشتر به دنبال ابزارهایی فنی مانند انواع آنتی‌ویروس‌ها، فایروال‌ها و... برای برطرف کردن مشکلات امنیتی‌شان بوده‌اند. گری هینسون (گری، ۲۰۰۳: ۸۰) بیان می‌کند که امنیت اطلاعات هم فناوری و هم فرد را دربرمی‌گیرد، اما بیشتر سازمان‌ها راه‌حل‌های فنی را جواب فوری به مشکلات امنیتی خود می‌دانند؛ در حالی که موانع زیادی در رویکرد فنی صِرف وجود دارد. سازمان‌ها باید مشکلات امنیتی خود را به خوبی و به طور کامل درک کنند تا بتوانند راه‌حل‌های فنی مناسب را بر اساس آن به کار گیرند؛ واژه «راه‌حل فنی» هزینهٔ زیادی دارد؛ فناوری‌های امنیتی صرف نظر از میزان اثربخشی‌شان، می‌توانند مورد استفادهٔ نادرست کاربران قرار گیرند یا دچار اختلال شوند که از این طریق سودمندی خود را از دست می‌دهند. بررسی‌های انجام‌شده نشان می‌دهد در خصوص عوامل انسانی مؤثر در امنیت اطلاعات تحقیقات اندکی انجام گرفته است. از سوی دیگر، آموزش و اطلاع‌رسانی کاربران یکی از پایه‌ها و سرفصل‌های اساسی برنامه‌های امنیتی است و جای خالی این مسئله در سازمان‌ها محسوس است. از این رو توجه به بُعد فردی در کنار بُعد فنی یا شاید با اهمیت‌تر از آن باید در برقراری امنیت سیستم‌های اطلاعاتی مد نظر قرار گیرد. بنابراین آنچه موجب دغدغه و نگرانی در این روند بوده و به عنوان چالشی اساسی مطرح است، عوامل و شاخص‌هایی هستند که عوامل انسانی را در موفقیت یا عدم موفقیت در مواجهه با سیستم‌های اطلاعاتی تحت تأثیر قرار می‌دهند که در این مقاله به آنها پرداخته می‌شود.

1 . Haiynd

پیشینه پژوهش و مبانی نظری

۱. تعاریف امنیت سیستم‌های اطلاعات

در تعاریف امنیت سیستم‌های اطلاعات، سه مؤلّفه به عنوان مبانی اصلی اثربخش در امنیت اطلاعات معرفی شده‌اند:

۱. محرمانه بودن تا فقط افراد مجاز حق دسترسی به اطلاعات را داشته باشند.

۲. صحت و استحکام تا اطلاعات دست‌نخورده بماند و تغییر در آنها توسط افراد مجاز در صورت لزوم به صورت درست و قابل پیگیری انجام شود.

۳. در دسترس بودن تا اطلاعات در موقع نیاز به صورت قابل استفاده در دسترس قرار گیرد (سرلک و فراتی، ۱۳۹۱: ۲۹۵).

دستیابی به این فاکتورها را اثربخشی امنیت سیستم‌های اطلاعاتی می‌نامند. به مسئله امنیت اطلاعات نیز از جنبه‌ها و زاویه‌های گوناگونی نگاه می‌شود. امنیت سیستم‌های اطلاعاتی را می‌توان از دو جهت بررسی کرد که عبارت‌اند از: فناوری و افراد.

۲. پایه و اساس امنیت سیستم‌های اطلاعاتی

ـ سیاست‌ها و دستورالعمل‌های امنیت: طرح‌ها و برنامه‌های مرتبط با نحوه محافظت از سیستم‌های اطلاعاتی و داده‌های آنها در این قسمت مورد توجه توجه قرار می‌گیرد. راهبرد امنیت در دو بخش غیرفنی و فنی ارائه می‌شود. بخش غیرفنی شامل تعیین دستورالعمل‌های لازم برای به کارگیری و نظارت بر اجزای سیستم امنیت جهت نیل به اهداف راهبردی است.

ـ فناوری و محصولات امنیتی: این قسمت شامل ابزارهای مورد استفاده در بخش‌های مختلف امنیتی برای اعمال دستورالعمل‌ها و اعمال کنترل‌ها و نظارت‌های امنیتی است. برخی از ابزارها و محصولات امنیتی شامل ابزارهای محافظتی و نظارت بر شبکه، سیستم‌های کنترل دسترسی و راهکارهای ضد ویروس است.

عوامل اجرایی: عوامل اجرایی مرتبط با امنیت سیستم‌ها و فناوری‌های اطلاعاتی شامل مدیران سیستم‌های اطلاعاتی و شبکه‌های ارتباطی، کارکنان و کاربران عادی این سیستم‌ها هستند. این عوامل از فناوری‌ها و ابزارهای پیشرفته برای اجرای سیاست‌ها و دستورالعمل‌های امنیتی استفاده می‌کنند. سازماندهی و مدیریت اجزای فوق نیاز به دستورالعمل‌ها و واحدهای اطلاعات را تحت پوشش قرار می‌دهد و با برقراری امکان نظارت و بهبود مستمر، امنیت کل مجموعه را تأمین می‌کند (سرلک و فراتی، ۱۳۹۱: ۲۷۹).

۳. عوامل انسانی و امنیت سیستم‌های اطلاعاتی

گونزالز عامل انسانی را پاشنهٔ آشیل امنیت اطلاعات معرفی کرده است (جوز و آگاتا، ۲۰۰۲: ۵۶). به گفته دیوید ماکی، رئیس بخش آگاهی شرکت کامپیوتری آرمونک، کاربر هم‌نان به عنوان سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیتی، مورد سوءاستفاده قرار خواهد گرفت. در سال ۲۰۰۴، باسی و راسوف مقاله‌ای را با عنوان «ده خطای مهلک مدیریت امنیت سیستم‌های اطلاعاتی» منتشر کردند (باسی و راسوف، ۲۰۰۴: ۳۷۱). آنها پس از بیان این ده خطای مهلک امنیت سیستم‌های اطلاعاتی در ادامه خاطرنشان کردند که حتی اگر یکی از این جنبه‌ها نادیده گرفته شود یا به درستی مورد توجه قرار نگیرد، مشکلاتی جدی در حفظ یک برنامه امنیت سیستم‌های اطلاعاتی وجود خواهد داشت. قسمت عمده‌ای از این خطاها مبتنی بر عوامل انسانی و مسائل مربوط به آنهاست. همچنین در سال ۲۰۰۶ مقاله‌ای با عنوان «امنیت اطلاعات، موج چهارم» به بررسی چهار موج امنیت اطلاعات تا کنون پرداخت. موج اول، موج فنی بود که به راه‌حل‌های فنی ارائه‌شده برای مسائل امنیتی مربوط می‌شد. دومین موج بیان می‌کرد که امنیت اطلاعات بُعد مدیریتی قوی‌ای دارد. آن ابعاد مانند خط‌مشی و درگیری مدیریت بسیار مهم‌اند. موج سوم از یک نیاز برای داشتن فرمی از استاندارد کردن امنیت اطلاعات در شرکت و جنبه‌هایی مانند بهترین تمرین‌های مدیریتی، تأیید یک فرهنگ مناسب امنیت اطلاعات و اندازه‌گیری و نظارت امنیت اطلاعات تشکیل شده است. موج چهارم نیز دربارهٔ توسعه نقش قطعی چگونگی ادارهٔ امنیت اطلاعات است (باسی، ۲۰۰۶: ۱۶۵). همه موارد یادشده باید با هم کار کنند تا این اطمینان حاصل شود که قابلیت اعتماد، تمامیت و در دسترس بودن دارایی‌های اطلاعاتی، در همه زمان‌ها، حفظ شده است (پورتال اینترنتی شرکت واترهاس، ۲۰۰۴: ۱۰).

همان‌طور که ملاحظه می‌شود، در اینجا نیز از موج اول به بعد، مباحث مدیریتی در امنیت اطلاعات نمایان‌تر شده و بر اساس جدیدترین موج امنیت اطلاعات که به تازگی منتشر شده، نقش مدیریت عالی، آموزش و آگاهی کاربر و خط‌مشی امنیتی به عنوان مبانی اصلی آن بیان شده است (ساپرونوف، ۲۰۰۵). به تازگی یک الگوی جدید نیز در زمینه امنیت اطلاعات به وجود آمده است که به آن در مقام یک مسئله انسانی و یک مسئله سازمانی توجه می‌شود (کناپ و همکاران، ۲۰۰۴: ۲۱). امروزه به نظر می‌رسد موفقیت امنیت اطلاعات تا حد زیادی به رفتار اثربخش کاربران وابسته است. رفتارهای درست و سازنده کاربران، مدیران سیستم و افراد دیگر می‌تواند اثربخشی

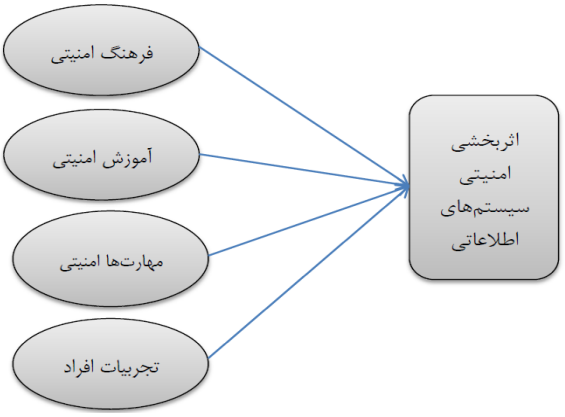
امنیت اطلاعات را تا حد زیادی بالا ببرد؛ در حالی که رفتارهای نادرست و مخرب ممکن است مانع اثربخشی آن شود (ساپرونوف، ۲۰۰۵). با توجه به موارد پیش‌گفته، جدول تحلیلی زیر می‌تواند به عنوان الگوی پیشنهادی برای شناسایی عوامل مؤثر بر اثربخشی امنیت سامانه‌های اطلاعاتی در جامعه آماری مطمح نظر قرار گیرد.

جدول ۱ــ خلاصه‌ای از مطالعات انجام‌شده

ردیف	مؤلفه	شاخص	نویسنده (سال)
۱	فرهنگ امنیتی	نگرش، سنت‌ها و ارزش‌ها	کنس و همکاران (۲۰۰۵)؛ چلیر و راسوف (۲۰۰۴)؛ اسچلینگر و تئوفل (۲۰۰۳)
۲	آموزش امنیتی	برنامه‌های آموزش امنیتی و ابزارهای آموزشی	سالوونا و همکاران (۲۰۰۵)؛ ماتیسن (۲۰۰۴)؛ تامپسون و سلمز (۱۹۹۸)؛ باسی و راسوف (۲۰۰۴)؛ کنس و همکاران (۲۰۰۵)
۳	مهارت امنیتی	دانش و نیت	مککلارس و فورنل (۲۰۰۵)؛ سی. ان.ان (۲۰۰۱)
۴	تجربیات افراد	تخصص افراد، توانایی‌های رایانه‌ای و زمان درگیر بودن در مباحث امنیتی	دانیل (۲۰۰۵)

مدل مفهومی و فرضیات تحقیق

در آغاز با استفاده از مطالعات کتابخانه‌ای و اکتشافی، مبانی نظری موضوع بررسی و سپس شناسایی مؤلفه‌ها و شاخص‌های متغیرها انجام شد و با توجه به بررسی‌های صورت‌گرفته، مدل مفهومی پژوهش در نمودار ۱ارائه شد.



شکل ۱ــ مدل مفهومی تحقیق

در راستای انجام این پژوهش فرضیه‌های زیر ارائه شد:

۱. بین فرهنگ امنیتی کاربر و اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای مثبت و معنادار وجود دارد.

۲. بین آموزش امنیتی کاربر و اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای مثبت و معنادار وجود دارد.

۳. بین مهارت‌های امنیتی کاربر و اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای مثبت و معنادار وجود دارد.

۴. بین تجربیات افراد و اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای مثبت و معنادار وجود دارد.

روش‌شناسی تحقیق

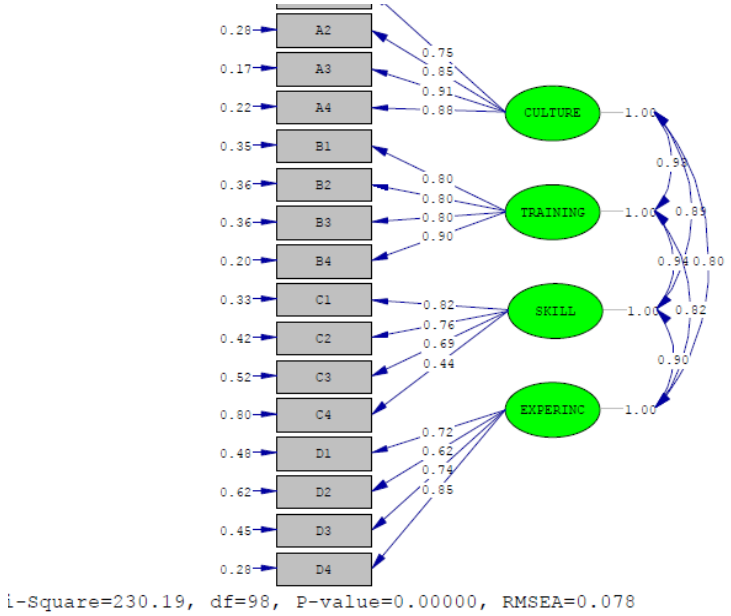
پژوهش حاضر از نظر هدف، کاربردی، از نظر ماهیت توصیفی- پیمایشی و از حیث روش همبستگی است. تحقیقات همبستگی شامل تمامی تحقیقاتی است که در آنها بین متغیرهای مختلف با استفاده از ضریب همبستگی کشف یا تعیین می‌شود. برای جمع‌آوری اطلاعات مربوط به ادبیات تحقیق و مباحث نظری مرتبط با موضوع از روش مطالعات کتابخانه‌ای (کتب فارسی و لاتین، مقالات و سایت‌های اینترنتی...) استفاده شده است. در این تحقیق برای تهیه پرسش‌نامه ابتدا متغیرهای فرعی شناسایی و به منظور بررسی دقیق‌تر، برای هر کدام از شاخص‌ها احصا شدند. سپس بر مبنای شاخص‌های تعیین‌شده، اقدام به طراحی سؤال‌ها شد. این پرسش‌نامه حاوی سؤال‌های جمعیت‌شناسی و ۲۴ پرسش مربوط به متغیرهای مورد بررسی است. همچنین به منظور پاسخ‌گویی به سؤال‌ها برای همه متغیرها از طیف ۵ مرتبه‌ای لیکرت از «بسیار کم تا بسیار زیاد» استفاده شده است. جامعه مورد مطالعه شامل همه کارشناسان و کاربران رایانه یکی از دانشگاه‌های نظامی سطح شهر تهران است که در سال ۱۳۹۳ مشغول فعالیت بودند. کارکنان این دانشگاه ۳۲۰ نفر بودند که ۱۷۵ نفر بر اساس جدول مورگان انتخاب شدند. نمونه‌گیری در این پژوهش با استفاده از روش نمونه‌گیری تصادفی ساده و به شکل طبقه‌ای انجام گرفت و نمونه‌ها به منظور تأمین پراکندگی مناسب و گویا بودن، از تمام دانشکده‌های موجود انتخاب شدند. برای تجزیه و تحلیل داده‌ها و برازش مدل معادلات ساختاری از نرم‌افزار اسمارت پی.ال.اس استفاده شد.

تحلیل عاملی مرتبه اول

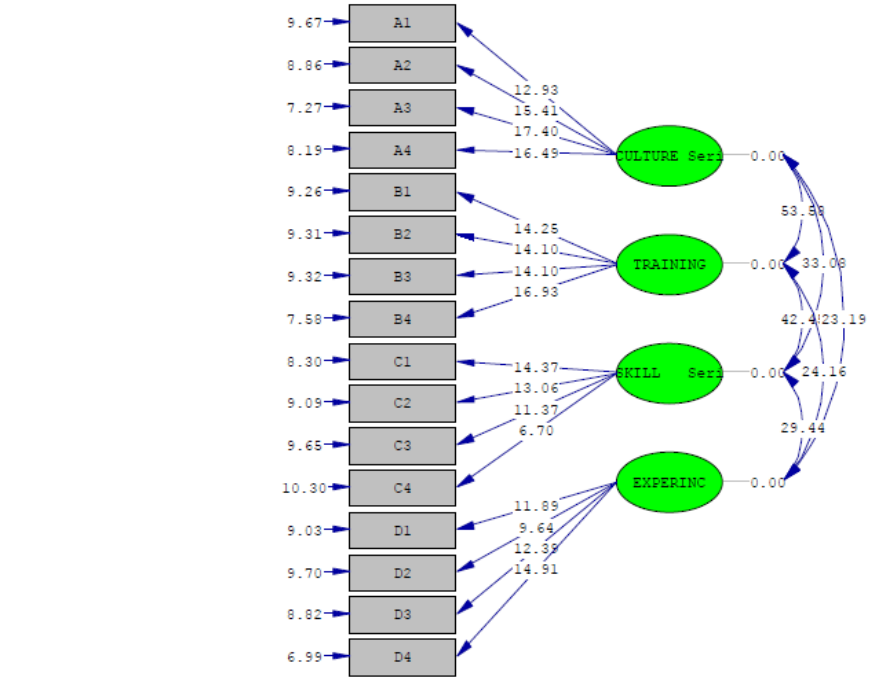
به منظور سنجش پایایی با استفاده از داده‌های به دست آمده از پرسشنامه، میزان ضریب اعتماد با روش آلفای کرونباخ محاسبه شد که نتایج پایایی متغیرهای «فرهنگ امنیتی»، «آموزش امنیتی»، «مهارت امنیتی» و «تجربیات افراد» به ترتیب ۰/۸۴۵، ۰/۸۳۱، ۰/۷۹۵ و ۰/۸۶۷ نشان داد. این اعداد گویای این است که پرسشنامه از قابلیت اعتماد و به بیان دیگر، از پایایی لازم برخوردار است. شایان ذکر است هیچ سؤالی به دلیل نامناسب بودن داده‌ها و عدم تبیین واریانس متغیر مربوط به آن، از مجموع سؤال‌ها حذف نشد. روایی سؤال‌ها نیز به کمک اعتبار عاملی سنجیده شد. اعتبار عاملی صورتی از اعتبار سازه است که از طریق تحلیل عاملی به دست می‌آید. تحلیل عاملی نوعی فن آماری است که در علوم انسانی کاربرد فراوانی دارد. در تحلیل عاملی اکتشافی، مقدار KMO، ۰/۸۷۱ به دست آمد که گویای کفایت نمونه‌گیری برای متغیرهای پژوهش است. همچنین از آنجا که ضریب معناداری آزمون بارتلت برابر صفر بود، تحلیل عاملی برای شناسایی ساختار، مناسب تشخیص داده شد. برای بررسی صحت مدل‌های اندازه‌گیری از تحلیل عاملی تأییدی استفاده شد. نتایج تمام بارهای عاملی بیشتر از ۰/۴ به دست آمد که روایی همگرای آن را نشان می‌دهد.

بررسی مدل‌های اندازه‌گیری متغیرهای پژوهش

قبل از وارد شدن به مرحلهٔ آزمون فرضیه‌ها و مدل‌های مفهومی پژوهش باید از صحت مدل‌های اندازه‌گیری متغیرهای پژوهش اطمینان حاصل کرد. از این رو در ادامه به بحث مدل‌های اندازه‌گیری متغیرهای پژوهش پرداخته می‌شود. این کار با بهره‌مندی از روش تحلیل عاملی تأییدی انجام شده است. نتایج تحلیل عاملی تأییدی متغیرهای پژوهش نشان می‌دهد تمام مدل‌های اندازه‌گیری و همهٔ اعداد و پارامترهای مدل مناسب و معنادارند. با توجه به اینکه تمام بارهای عاملی در تمام ابعاد بزرگ‌تر از ۰/۵ میانگین واریانس‌های استخراجی است و میانگین واریانس‌های استخراجی بیشتر از ۰/۵ به دست آمده است، بین سازه‌ها روایی همگرا وجود دارد. شکل‌های ۲ و ۳نتایج تحلیل عاملی را نشان می‌دهد. همان‌طور که مشاهده می‌شود، ابعاد از نظر شاخص‌های تناسب، در وضعیت مناسبی هستند.



شکل ۲ـ تحلیل عاملی مرتبه اول در حالت ضریب استاندارد



شکل ۳ـ تحلیل عاملی مرتبه اول در حالت ضریب معناداری

نتایج تحلیل عاملی تأییدی مرتبه اول (تحلیل عاملی پرسش‌نامه) نشان می‌دهد همه سؤال‌ها از روایی مناسبی برای سنجش متغیرهای پژوهش برخوردارند. معیار تأیید یا رد سؤال برای سنجش هر متغیر، اعداد معناداری بزرگ‌تر از ۱/۹۶ یا کوچک‌تر از ۱/۹۶- نشان می‌دهد آن سؤال برای سنجش بعد مد نظر مناسب است و چنانچه عدد معناداری در بازه یادشده باشد، آن سؤال برای سنجش مناسب نیست.

بررسی شاخص‌های برازش مدل

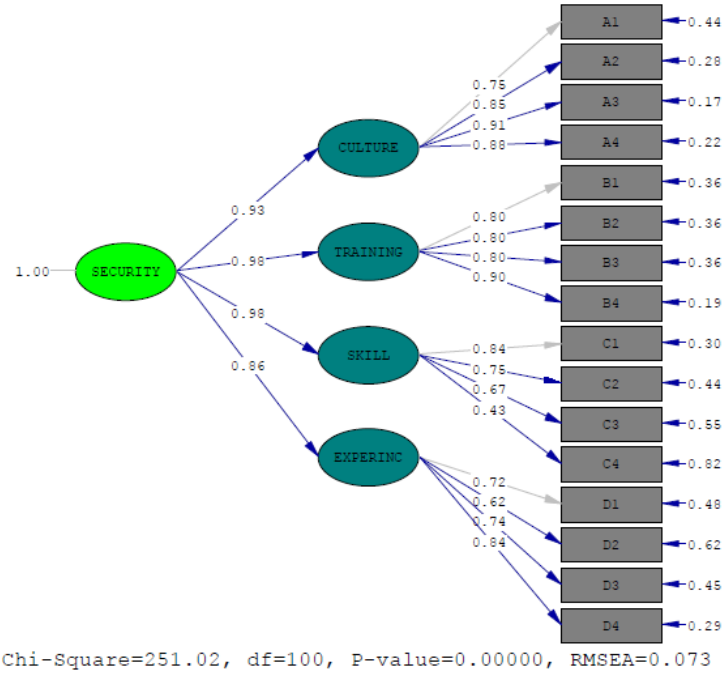
برای بررسی برازش متغیرها و مؤلفه‌های آن با داده‌های جمع‌آوری‌شده، از نرم‌افزار لیزرل ۸/۵۴ استفاده می‌شود. شاخص‌های برازش در جدول ۲ نشان داده شده است. شاخص کی‌دو اختلاف میان مدل و داده‌ها را نشان می‌دهد؛ بنابراین هر چه مقدار آن کمتر باشد، حاکی از اختلاف کمتر بین ماتریس واریانس- کواریانس نمونه و ماتریس واریانس- کواریانس حاصل از مدل است. به علت آنکه این شاخص تحت تأثیر تعداد نمونه قرار می‌گیرد، از تقسیم این شاخص بر درجه آزادی استفاده می‌شود. شاخص میانگین مجذور خطاهای مدل (RMSA) از شاخص‌های مهم در برازش مدل است. این شاخص بر اساس خطاهای مدل ساخته می‌شود و هر چه کمتر باشد، بهتر است. شاخص نیکویی برازش (GFI) نشان‌دهنده اندازه‌ای از مقدار نسبی واریانس‌ها و کواریانس‌هاست که توسط مدل تعیین می‌شود و هر چه بیشتر باشد، بهتر است. شاخص AGFI همان نیکویی برازش است که با در نظر گرفتن درجه آزادی تعدیل شده است. شاخص نرم‌شده برازندگی (NFI) یکی دیگر از شاخص‌های برازش مدل است که مقادیر بالای آن بهتر است.

جدول ۲ـ اطلاعات مربوط برازش کلی مدل تحقیق

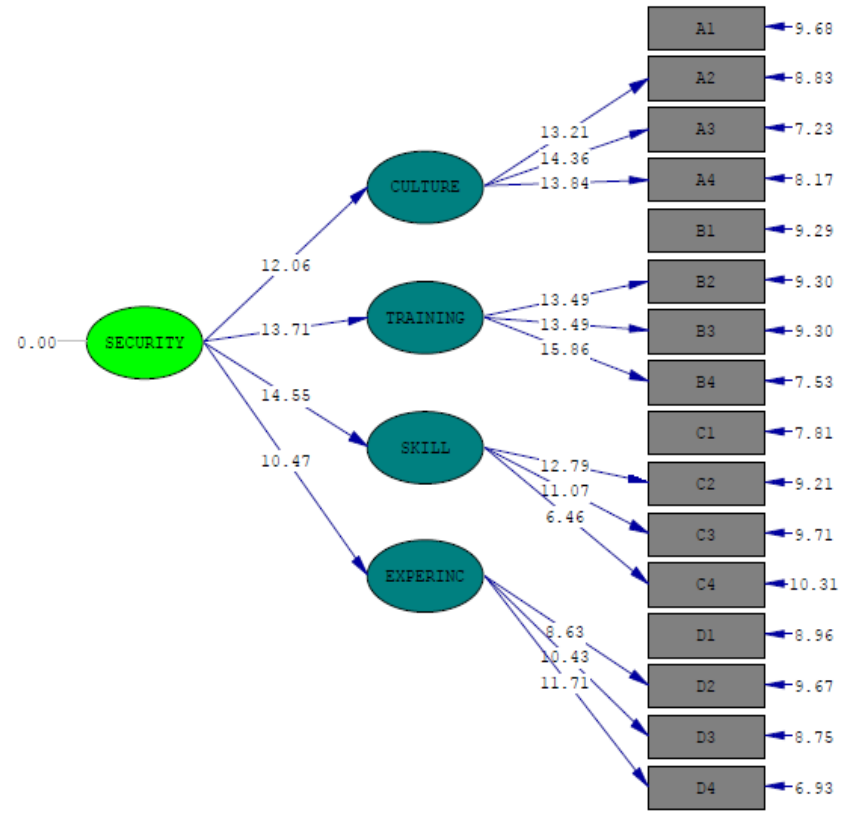
نام پارامتر	مقدار	حد مجاز
نسبت کای اسکوئر به درجه آزادی	۲/۵۱	کوچک‌تر از ۳
شاخص برازش غیرنرم (NNFI)	۰/۹۴	بزرگ‌تر از ۰/۹
شاخص برازش تطبیقی (CFI)	۰/۹۳	بزرگ‌تر از ۰/۹
شاخص برازش افزایشی (IFI)	۰/۹۴	بزرگ‌تر از ۰/۹
شاخص برازندگی (GFI)	۰/۹۲	بزرگ‌تر از ۰/۹
شاخص برازندگی تعدیل‌یافته (AGFI)	۰/۹۰	بزرگ‌تر از ۰/۹

مأخذ: نتایج پژوهش

مقایسه میان مقدار شاخص‌ها با حد مجاز در نظر گرفته‌شده برای آنها، نشان‌دهنده برازش مدل در نظر گرفته‌شده برای متغیرها با داده‌های جمع‌آوری‌شده است. اکنون با مدل مفهومی پژوهش و با استفاده از مدل‌سازی معادلات ساختاری، به طور اخص تکنیک تحلیل مسیر، به بررسی فرضیات پرداخته می‌شود. تحلیل مسیر، تکنیکی است که روابط بین متغیرهای تحقیق را به‌طور هم‌زمان نشان می‌دهد. بدین منظور از نرم‌افزار لیزرل نسخه ۸/۵۰ استفاده شده است. دو خروجی مهم نرم‌افزار، مدل در حالت تخمین استاندارد و مدل در حالت ضرایب معناداری است. در حالت تخمین استاندارد میزان تبیین استاندارد میزان تبیین واریانس هر متغیر توسط متغیرهای وابسته به آن مشخص می‌شود و در خروجی ضرایب معناداری، معنادار بودن روابط متغیرها مشخص می‌گردد. اگر ضرایب معناداری (مقدار آماره t) بیش از ۱/۹۶ یا کمتر از ۱/۹۶- باشد، مقدار واریانس تبیین‌شده معنادار است. شکل‌های ۴ و ۶ دو خروجی نرم‌افزار را نشان می‌دهند. با توجه به میزان اثر متغیرها بر یکدیگر و با در نظر گرفتن ضرایب معناداری این روابط، می‌توان به تأیید یا رد فرضیات پرداخت. جدول ۳ خلاصه‌ای از نتایج را نشان می‌دهد.



شکل ۴ـ مدل ساختاری در حالت ضریب استاندارد



شکل ۵ـ مدل ساختاری در حالت ضریب معناداری

نتایج ارائه‌شده در جدول ۳ نشان‌دهنده اثر مثبت و معنادار شاخص‌های احصا شده است.

جدول ۳ـ نتایج آزمون فرضیه اصلی تحقیق

فرضیه	مقدار بار عاملی	مقادیر معناداری	نتیجه
بین فرهنگ امنیتی کاربر و اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای مثبت و معنادار وجود دارد.	۰/۹۳	۱۲/۰۶	تأیید
بین آموزش امنیتی کاربر و اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای مثبت و معنادار وجود دارد.	۰/۹۸	۱۳/۷۱	تأیید
بین مهارت‌های امنیتی کاربر و اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای مثبت و معنادار وجود دارد.	۰/۹۸	۱۴/۵۵	تأیید
بین تجربیات افراد و اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای مثبت و معنادار وجود دارد.	۰/۸۶	۱۰/۴۶	تأیید

بحث و نتیجه‌گیری

هدف این پژوهش مطالعه و بررسی رابطه بین اثربخشی امنیت سیستم‌های اطلاعاتی با فرهنگ امنیتی، آموزش امنیتی، مهارت‌های امنیتی و تجربیات افراد بود. مرور پیشینه نشان داد که عوامل فوق می‌توانند در بهبود اثربخشی امنیت سیستم‌های اطلاعاتی نقش داشته باشند.

براساس یافته‌های تحقیق، فرهنگ امنیتی با اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای معنادار و مثبت دارد و این عامل در رتبه اول قرار دارد. امنیت کارآ نه تنها نیازمند برقراری ساختار سازمانی مناسب و انتشار قوانین و دستورالعمل‌های اجرایی است، بلکه نیازمند تعهد واقعی و عزم راسخ مدیران عالی است. نشانه‌های اولیه تعهد سازمانی در خصوص سیاست‌های امنیتی سازمان در فرهنگ امنیتی تجلی پیدا می‌کند. فرهنگ امنیتی عاملی است که به موجب آن تمامی کارکنان، متعهد می‌شوند سهم به‌سزایی در امنیت خود و همکاران‌شان داشته باشند. به بیان دیگر، در جهت ایجاد فرهنگ امنیتی مناسب باید تغییراتی مناسب در نگرش، سنت‌ها و ارزش‌های کارکنان ایجاد کرد تا بتوان بر رفتار و اندیشه اعضای سازمان نفوذ کرد و از این راه حرکت و پویایی را در سازمان به وجود آورد.

یافته‌های تحقیق نشان داد که آموزش امنیتی با اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای معنادار و مثبت دارد و در رتبه دوم از نظر اهمیت قرار دارد. با توجه به اهمیت نیروی انسانی، بعد از تدوین و تصویب سیاست‌های کلی سازمان باید تمامی کاربران از مفاد آن مطلع شوند و در صورت نیاز با برقراری جلسه‌های توجیهی، سطح آگاهی کاربران ارتقا یابد. بنابراین، برای اجرای سیاست‌های امنیت اطلاعات، آگاهی دادن به کاربران، از کارهای بسیار حیاتی و لازم است. کاربران و سایر کسانی که به منابع اطلاعاتی دسترسی دارند به واسطه بی‌دقتی یا آگاهی نداشتن از توانایی، پیش‌بینی خطرها را ندارند. به همین دلیل بهره‌گیری از فنون جلب توجه که شامل آموزش و ترویج تکنیک‌های حفاظت و ایجاد حساسیت در کاربران به منظور جلوگیری از افشای اطلاعات بر اساس سیاست‌های تدوین‌شده است، بسیار مفید خواهد بود.

یافته‌های تحقیق نشان داد مهارت‌های امنیتی با اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای معنادار و مثبت دارد. تحولات فناورانه و سازمانی مهارت‌های سازمانی را به سرعت منسوخ می‌کند. آموزش فرایندی است که از طریق آن کارکنان، توانایی بازتعریف پیوسته مهارت‌های لازم را برای یک کار معین و دسترسی به منابع یادگیری این مهارت‌ها را به دست می‌آورند. هر کسی که در محیط سازمانی مناسب

تعلیم می‌بیند، می‌تواند خود را متناسب با وظایف دائماً در حال دگرگونی فرایند تولید تنظیم کند. از سوی دیگر، کارکنان به اطلاعات و دانشی سوای توانایی دریافت و اجرای علایم نیازی ندارند. به بیانی دیگر، بشر امروز نیازهای فنی خود را متناسب با فناوری‌های روز در حد بالا می‌بیند و به صورتی دنیای امروز را ترسیم می‌کند که در همه بخش‌ها، مهارت‌های فنی و حرفه‌ای حرف اول را می‌زند.

یافته‌های تحقیق نشان داد که تجربیات افراد با اثربخشی امنیت سیستم‌های اطلاعاتی رابطه‌ای معنادار و مثبت دارد. شیوه‌ها و فنون خاصی که ما به خوبی آنها را فراگرفته‌ایم، جاودانه نخواهند بود و طول عمری دارند که به زودی سپری خواهد شد. بنابراین بالیدن به تاج‌های افتخار گذشته و تلاش نکردن برای یادگیری و تغییر مداوم نگرش‌ها اشتباه محض است. در چنین شرایطی هیچ فردی حتی نخبه‌ترین، باسوادترین و با تجربه‌ترین افراد به تنهایی قادر به تولید یا کسب دانش مورد نیاز خود با سرعت و شرایط مطلوب برای تطبیق دادن خود با شرایط کنونی عصر دانش‌محور امروز نیست و تنها چاره کار برای به‌روز ماندن افراد، تیم‌ها و سازمان‌ها و بقای آنها تلاش برای یادگیری تیمی و سازمانی و بهره‌مندی از سامانه‌های مدیریت دانش، پیوستن به این سامانه‌ها و تولید و انتشار دانش و استفاده از دانش و تجربیات همکاران دیگر است. در مدیریت دانش ما با هم و از یکدیگر می‌آموزیم و بدین ترتیب سرعت و کیفیت یادگیری ما در حد درخور توجهی افزایش می‌یابد و بقای ما و سازمان ما تضمین می‌شود. مدیریت دانش به ما می‌آموزد که از دیگران یاد بگیریم و دانسته‌های خود را با دیگران در میان بگذاریم و به رشد و پرورش یکدیگر بپردازیم و تکرار مکررات نکنیم.

منابع فارسی

ـ سرلک، محمدعلی و حسن فراتی (۱۳۹۱)، **سیستم‌های اطلاعات مدیریت پیشرفته**، تهران: انتشارات دانشگاه پیام نور.

- صنیعی، محمدحسین (۱۳۹۲)، «فناوری اطلاعات و ارتباطات و امنیت آن»، **فصلنامه مطالعات حفاظت و امنیت انتظامی**، ۲۸(۸).

منابع لاتین

- Ammeter A, Douglas C, Gardner W, Hochwarter W, Ferris G (2002), "Toward a Political Theory of leadership", ***The Leadership Quarterly***, 13:751e96.

- Bagchi, K. and G. Udo (2004), "An Analysis of the Growth of Computer and Internet Security Breaches", ***Communications of the AIS***, 2003. 12(46).

- Carley, Kathleen M. (2000), "Information Security: The Human Perspective, Dept. of Social and Decision Sciences", Carnegie Mellon University, August.

- CNN.com. The Case against Robert Hanssen, In-depth Special Series, http://edition.cnn.com/SPECIALS/hanssen, 2001.October 25, 2005.

- Computer Emergency Response Team (CERT) (2004),CERT Statistics.

- Cronbach, L. (1951), "Coefficient Alpha and the Internal Structure of Tests", Psychometrika.

- Danielc, Phelps (2005), Information System Security: Self-efficacy and Security Effectiveness in - Florida Libraries, A Dissertation Submitted to the College of Information in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy, Spring Semester.

- Fornell, C & ,.Larcker, D.(1981), "Evaluating Structural Equation Models with Unobservable and Measuring Error", ***Journal of High Technology Management Reasearch***.۵۰-۳۹ ,

- G.B. Magklaras, S.M. Furnell (2005), "A Preliminary Model of End User Sophistication for Insider Threat Prediction", in ***IT Systems Computers & Security***, 24.

- Gonzalez, Jose J (2002), Agata Sawicka, A Framework for Human Factors in Information Security, Dept. of Information and Communication Technology, Agder University College, Presented at the 2002 WSEAS Int. Conf. on Information Security, Rio de Janeiro.

- Gordon, L.A., et al.(2004), "9th Annual CSI/FBI Computer Crime and Security Survey", Computer Security Institute: San Francisco, CA.

- Hensler, J., Ringle, C & Sinkovics, R. (2009), "The Use of Patial least Square Based Multi Group Analysis": In .advance in international marketing 20.

- Hinson, Gary, IsecT Ltd (2003), "Human Factors in Information Security", ***Innovative Information Security Awareness Programs***, NoticeBored.

- Hulland, j (1999), "Use of Partial least Squres in Stratgic Management Research": a review of four recent studies .stratgic management journal.20- 195.

- M.E. Thomson and R. von Solms (1998), "Information Security Awareness: Educating Your Users Effectively", ***Information Management & Computer Security*** 6/4.

- Mathisen, J.(2004), ***Measuring Information Security Awareness***, Høgskolen i Gjøvik.

- Nelson DL, Jepson-Thomas J. (2003), "Occupational form,

Occupational Performance, and a Conceptual Framework for Therapeutic Occupation", Perspectives in Human Occupation: Participation in life, Philadelphia: lippincott Williams & Wilkins.

- Nunnaly, J & Bernsten, I. (1994), ***Psychometric Theory,*** New york: Mc Graw Hill.

- Nunnaly, J.C و .Bernsten (1994), ***I.H. Psychometric Theory***, New york : Mc Graw Hill.

- Orshesky, C. (2003), "Beyond Technology - The Human Factor in Business Systems", ***Journal of Business Strategy***, 24, 4.

- Salanova, M., Grau, R. M., Cifre, E., & Llorens, S. (2000), "Computer Training, Frequency of Usage and Burnout: The Moderating Role of Computer Self-efficacy", ***Computers in Human Behavior***, 16.

- Sapronov, K., (2005)," The Human Factor and Information Security", Available:ttp://www.securelist.com/en/analysis?pubid=176195190 [accessed: 12 July 2012].

- Schlienger, T. and S. Teufel (2003), Analyzing Information Security Culture: Increasing Trust by an Appropriate Information Security Culture, Unpublished, Accepted on the TrustBus' Workshop in Conjunction with the 14th International Conference on Database and Expert Systems Applications (DEXA 2003).

- Schou, C.D. and K.J. Trimmer(2004), "Information Assurance and Security", ***Journal of Organizational and End User Computing***, 16(3).

- Solmsa, Basie von, Rossouw von Solms (2004), "The 10 Deadly Sins of Information Security Management", ***Computers & Security***, 23.

- Theoharidou, Marianthi, Spyros Kokolakis, Maria Karyda, Evangelos Kiountouzis (2005), "The Insider Threat to Information Systems and the Effectiveness of ISO17799", ***Computers & Security***, 24.

- Thomson, K., & Van Niekerk, J. (2012), "Combating Information Security Apathy by Encouraging Prosocial Organisational Behavior", ***Nformation Management & Computer Security***, 20, 1.

- Vroom ,Cheryl, Rossouw von Solms(2004), "Towards Information Security Behavioral Compliance", ***Computers & Security***, 23.