ارائهٔ چارچوبی برای عوامل انسانی مرتبط در امنیت سیستم‌های اطلاعاتی

شعبان الهی[1*]، مهدی طاهری[2]، علیرضا حسن زاده[3]

۱- استادیار گروه مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران
۲- دانش آموخته کارشناسی ارشد رشته مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران
۳- استادیار گروه مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران

دریافت: ۸۶/٤/۱۷ پذیرش: ۸۷/۲/٤

چکیده

امنیت اطلاعات یک مسألهٔ حیاتی است و امروزه سازمان‌ها در سراسر دنیا با آن روبه‌رو هستند. امنیت سیستم‌های اطلاعاتی[1] هم فناوری و هم افراد (عوامل انسانی) را در برمی‌گیرد. در بیشتر تحقیقاتی که در زمینهٔ امنیت سیستم‌های اطلاعاتی صورت گرفته؛ یک نوع دید و رویکرد فنی وجود داشته است. پژوهش حاضر در راستای الگوی جدیدی است که آن را "مسأله انسانی" و"مسأله سازمانی" می‌نامند. این الگو بر "امنیت اطلاعات رفتاری" تمرکز دارد و در آن بر این نکته که کاربران و در کل عوامل انسانی، ضعیف‌ترین و سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیت سیستم‌های اطلاعاتی مطرحند تأکید می‌شود. در این پژوهش با در نظر گرفتن اهمیت امنیت، برای سازمان‌های امروزی، یک مدل مدیریتی برای بررسی نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی ارائه می‌شود. هدف این پژوهش، به طور خاص شناسایی و مدل‌سازی سازه[2]های مدیریتی حیاتی و اساسی مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی است. در این راستا، سازه‌های "حمایت مدیریت عالی، آموزش امنیتی، فرهنگ امنیتی، مهارت امنیتی، تقویت خط‌مشی امنیتی، تجربیات و خودباوری افراد" به‌عنوان فاکتورهای مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی معرفی می‌شوند. روش‌شناسی این

---

* نویسندهٔ مسؤول مقاله: elahi@modares.ac.irEmail:

1. Information Systems Security
2. Construct

مطالعه، ترکیبی از تکنیک‌های کیفی و کمّی تحقیق است. از طریق تکنیک‌های کیفی و بررسی پیشینهٔ موضوع، متغیرهای کلیدی مؤثر بر امنیت سیستم‌های اطلاعاتی شناسایی شده‌اند.

سپس با توجه به مدل مفهومی پژوهش که از مرور پیشینه و منابع موضوع و بررسی نتایج تحقیقات قبلی به‌دست آمده است، ابزار جمع‌آوری داده‌ها (پرسشنامه) طراحی شده و نسبت به جمع‌آوری داده‌ها از طریق نمونه‌های انتخابی (خبرگان و سازمانی) اقدام شده است. پس از آن داده‌های جمع‌آوری شده توسط SPSS و LISREL مورد تجزیه و تحلیل قرار گرفته‌اند و طبق آن، مدل نهایی تحقیق با عنوان " مدل عوامل انسانی مؤثر بر امنیت سیستم‌های اطلاعاتی" ارائه شده است.

کلید واژه‌ها: سیستم‌های اطلاعاتی، امنیت سیستم‌های اطلاعاتی، اثربخشی امنیتی، سازه‌های مدیریتی.

۱- مقدمه

در تجارت امروز، اطلاعات نقش سرمایهٔ یک شرکت را ایفا می‌کند و حفاظت از اطلاعات و سیستم‌های اطلاعاتی سازمان، یکی از ارکان مهم بقای آن می‌باشد. جهانی شدن اقتصاد، باعث ایجاد رقابت در سطح جهانی شده است و بسیاری از شرکت‌ها برای ادامهٔ حضور خود در عرصهٔ جهانی، ناگزیر به همکاری با سایر شرکت‌ها هستند. به این ترتیب، طبقه‌بندی و ارزش‌گذاری و حفاظت از منابع اطلاعاتی سازمان (چه در مورد سیستم اطلاعاتی و چه اعضای سازمان) بسیار حیاتی و مهم است.

با توجه به اقتصادهای ملی مدرن که کاملاً برای بقا به فناوری اطلاعات[1] وابسته شده‌اند، امروزه نیاز به امنیت اطلاعات وسیستم‌های اطلاعاتی اجتناب‌ناپذیر است. طبق این شرایط نیاز به حمایت از اطلاعات و کاهش ریسک نسبت به قبل بسیار مهم‌تر و برجسته‌تر شده است [۱، صص ۱۲۳-۱۴۵]. بررسی‌های ملی متعدد، تعداد زیادی از حملات به منابع اطلاعاتی سازمان را تطبیق داده‌اند [۲، صص ٦٨٤-٧٠٠؛ ۳، صص ۷۵۱-۹٦؛ ٤، صص ۱-۲؛ ۵، صص ۱۱۸-۱۲۹]. بین سال‌های ۱۹۹۸ و ۲۰۰۳، تعداد حوادث گزارش شده به " تیم پاسخ به شرایط اضطراری کامپیوتری آمریکا، تقریباً هر سال دو برابر شده است، که باید به آن تعداد ۱۳۷, ۵۲۹ حادثه‌ای را که تنها در سال ۲۰۰۳ گزارش شده نیز اضافه کرد. بر طبق تحلیل ارنست و یانگ[2]، حوادث

1. Information Technology
2. Ernst and Young

امنیتی برای هر رخداد می‌تواند هزینه‌ای بین ۱۷ و ۲۸ میلیون دلار برای شرکت‌ها داشته باشد. از آن‌جا که حوادث، مکرر و هزینه‌بر هستند، مدیریت باید امنیت را به‌صورت جدی مورد توجه قراردهد تا بتواند اطلاعات و سیستم‌های اطلاعاتی سازمانی را حفظ و حمایت کند.

۲- بیان مسأله

در سال ۱۹۸۰، مجلهٔ ام ای اس[1] نتایج یک بررسی مسایل کلیدی را که به تعدادی از اعضای جامعهٔ مدیریت اطلاعات[2] و یک گروه از مدیران اجرایی فناوری اطلاعات داده شده بود، منتشر کرد. طی دههٔ ۱۹۸۰ امنیت به‌عنوان یک مسأله ردهٔ پایین رتبه‌بندی شد و هرگز رتبه‌ای بیشتر از ۱۲ کسب نکرد [٦، ص١٦]. در بررسی ۱۹۹٤ امنیت کاملاً از لیست ۲۰ مسألهٔ بالا جدا شد. با وجود این در بررسی‌ای که در سال ۲۰۰۳ انجام شد، امنیت و حریم خصوصی نوسان زیادی پیدا کرد تا جایی که در میان شرکت‌کنندگان در این بررسی به‌عنوان سومین مسأله با درجهٔ اهمیت زیاد شناسایی شدند. جدول (۱) خلاصه‌ای از اینکه چگونگی رتبه‌بندی مسائل امنیتی در طی سال‌های ۱۹۸۰ تا ۲۰۰۳ را نشان می‌دهد.

جدول۱ نتایج رتبه‌بندی از مسألهٔ امنیت [۶، ص۱۶]

رتبه	سال
۱۲	۱۹۸۰
۱۸	۱۹۸٦
۱۹	۱۹۸۹
سقوط کرد	۱۹۹٤
۳	۲۰۰۳

با بررسی جدول بالا به نظر می‌رسد که مدیران اجرایی IT ، امروزه امنیت را به‌عنوان یکی از مسائل عمدهٔ خود می‌بینند. امنیت اطلاعات و سیستم‌های اطلاعاتی یک مسألهٔ حیاتی

1. MIS Quarterly
2. Society of Information Management

است که امروزه سازمان‌ها در سراسر دنیا با آن روبه‌رو هستند. معمولاً در تعاریف امنیت سیستم‌های اطلاعات، سه مؤلّفهٔ به‌عنوان مبانی اصلی اثربخش در امنیت اطلاعات معرّفی می‌شوند:

- **قابلیت اعتماد**: اطمینان یافتن از اینکه اطلاعات تنها برای آنهایی که مجاز به دستیابی‌اند، در دسترس است.
- **تمامیت (انسجام)**: محافظت کردن از درستی و کامل‌بودن اطلاعات و روش‌های پردازش.
- **در دسترس بودن**: اطمینان یافتن این‌که کاربرانِ مجاز، به‌هنگام نیاز، به اطلاعات و دارایی‌ها دست می‌یابند. دستیابی به این فاکتورها را اثربخشی امنیت سیستم‌های اطلاعاتی می‌نامند. به مسأله امنیت اطلاعات نیز از جنبه‌ها و زاویه‌های گوناگونی نگاه می‌شود. امنیت سیستم‌های اطلاعاتی را می‌توان از دو جهت بررسی کرد که عبارتند از: فناوری و افراد.

تاکنون بیشترین تحقیقاتی که در زمینهٔ امنیت سیستم‌های اطلاعاتی[1] (ISS) انجام شده، در زمینهٔ مسائل فنی و تاکتیکی بوده است و در نتیجه نگرش و دیدن ISS به‌عنوان یک مسألهٔ فنی بر تحقیقات و تمرین‌های تحقیقاتی ISS تسلّط داشته است [۷، صص ٦٢-٧٣؛ ۸، صص ٤٣؛ ۹، صص ٧٦-٨٦؛ ۱۰، صص ٤٣-٥٠؛ ۱۱، صص ٤٨٢-٤٨٤؛ ۱۲، صص ٣٤-٣٦]. هایند[2] (۲۰۰٤) بیان می‌کند که در بیشتر تحقیقاتی که در زمینه ISS صورت گرفته است یک نوع دید و رویکرد فنی وجود داشته است و متخصصین امنیت اطلاعات بیشتر به‌دنبال یک سری ابزارهای فنی مانند انواع آنتی‌ویروس‌ها، فایروال‌ها و... برای برطرف کردن مشکلات امنیتی‌شان بوده‌اند. گری هینسون[3] [۱۲، صص۸۰-۸۱] بیان می‌کند که امنیت اطلاعات هم تکنولوژی و هم فرد را دربر می‌گیرد، امّا بیشتر سازمان‌ها راه‌حل‌های فنی را جواب فوری به مشکلات امنیتی خود می‌دانند، در حالی‌که موانع زیادی برای یک رویکرد فنی صرف وجود دارد از جمله:

۱. تکنولوژی جایز الخطا است؛

۲. سازمان‌های کمی باید مشکلات امنیتی خود را به‌خوبی و به‌طور کامل درک کنند تا بتوانند راه حل‌های فنی مناسب را براساس آن به‌کار گیرند؛

1. Information System Security
2. Haiynd
3. Gary Hinson

۳.واژه "راه حل فنی" هزینهٔ زیادی را دربر می‌گیرد؛

٤.تکنولوژی‌های امنیتی جدای از میزان اثر بخشیشان، می‌توانند مورد استفادهٔ نادرست کاربران قرار گرفته یا دچار اختلال شوند که از این طریق سودمندی خود را از دست می‌دهند.

در زمینهٔ امنیت اطلاعات، مطالعات کمی انجام شده‌است که در آنها مدل‌هایی به‌صورت تجربی تست شده و محدودیت‌ها و سازه‌های مربوط به رفتار وعوامل انسانی و یا سازه‌های سازمانی و مدیریتی به‌کار گرفته شده باشد و اگرهم تحقیقاتی در این زمینه انجام شده، به رفتار افراد در آنها توجه نشده، بلکه به نتایج رفتاری توجه شده است [۱۳، صص۵۹۷-٦۰۷؛ ١٤، صص۲۷۱-۲۷۳؛ ۱۵، صص۲-۹]. بیشتر دانشمندان و متخصصان امنیت اطلاعات، بر کمبود انجام تحقیقات تجربی جدّی در این زمینه‌ها تأکید کرده‌اند [١٦، صص٦۹۰-٦۹۲؛ ۱۷، صص٦۷۸-٦۹۰؛ ۱۸، صص٦۰۱-٦۰۳]. در ایران نیز با کمی ارفاق می‌توان گفت هیچ‌کس وضعیت فعلی خود را نمی‌شناسد؛ اکنون از کاربران خانگی یا شرکت‌های خصوصی توقعی نیست؛ اما کدام سازمان دولتی را می‌شناسیم که حداقل تصور قابل دفاعی از وضعیت گذشته و دورنمای امنیت سیستم‌ها و منابع اطلاعاتی خود داشته باشد. آموزش و اطلاع‌رسانی کاربران یکی از پایه‌ها و سرفصل‌های اساسی برنامه‌های امنیتی است و جای خالی این مسأله در سازمان‌های دولتی به‌شدت محسوس است. با توجه به اهمیت فزآیندهٔ عوامل انسانی در سیستم‌های اطلاعاتی و امنیت آن، نیاز به اجرای یک پژوهش گسترده و جامع در این زمینه احساس می‌شود.

تحقیق حاضر، رویکرد متفاوتی را به امنیّت اطلاعات با تمرکز بر "امنیت اطلاعات رفتاری[1]" ارائه می‌دهد. این رویکرد دربارهٔ آن دسته از پیچیدگی‌های عوامل انسانی است که بر در دسترس بودن، قابلیت اعتماد و تمامیت سیستم‌های اطلاعاتی مؤثر است. بنابراین با توجه به جای خالی یا کمبود عمومی پژوهش تجربی و اهمیّت امنیت اطلاعات برای سازمان‌های امروزی، این مطالعه در جست و جوی شناسایی و مدل‌سازی سازه[2]های مدیریتی حیاتی و اساسی مؤثر بر اثربخشی امنیت اطلاعات در سازمان است.

---

1. Behavioural Information Security
2. Construct

۳- عوامل انسانی و امنیت سیستم‌های اطلاعاتی

گونزالز عامل انسانی را به‌عنوان پاشنهٔ آشیل امنیت اطلاعات معرفی کرده است [۱۰، ص۵۶]. IBM بیان کرده است که سال ۲۰۰۶ ضمن این‌که حملاتِ کوچک‌تر، متمرکزتر و پنهان‌کارانه‌تری به سیستم‌های اطلاعاتی سازمان‌ها صورت خواهد گرفت، کانون توجه نفوذگران، "*سهل انگاری و ساده اندیشی کاربران*" خواهد بود. به گفته دیوید ماکی، رئیس بخش آگاهی شرکت کامپیوتری آرمونک[1]، "کاربر" همچنان به‌عنوان *سست‌ترین عنصر* آسیب‌پذیر در مدل‌های امنیتی، مورد سوء استفاده قرار خواهد گرفت. در سال ۲۰۰۴ دو محقق، مقاله‌ای با عنوان "ده خطای مهلک مدیریت امنیت سیستم‌های اطلاعاتی" را منتشر کردند [۱۸، صص۳۷۱-۳۷۶]. در این مقاله ده خطای زیر به‌عنوان خطاهای مهلک ISS ذکر شدند و بیان شد که حتی اگر یکی از این جنبه‌ها نادیده گرفته شود و یا به‌درستی مورد توجه قرار نگیرد، مشکلاتی جدی، در حفظ یک برنامه ISS وجود خواهد داشت. قسمت عمده‌ای از این خطاها مبتنی بر عوامل انسانی و مسائل مربوط به آنها می‌باشد.

همچنین در سال در ۲۰۰۶ مقاله‌ای با عنوان "امنیت اطلاعات، موج چهارم" به بررسی چهار موج امنیت اطلاعات تا کنون پرداخته شده است [۱۹، صص۱۶۵-۱۶۸]. موج اول *موج فنی*[2] بود که به راه‌حل‌های فنی ارائه شده برای مسائل امنیتی مربوط می‌شد. دومین موج بیان می‌کرد که امنیت اطلاعات بعد مدیریتی[3] قوی‌ای دارد. آن ابعاد مانند خط‌مشی و درگیری مدیریت بسیار مهم‌اند. موج سوم از یک نیاز برای داشتن فرمی از *استاندارد کردن*[4] 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*[5] است.

همه موارد یاد شده باید با هم کار کنند تا این اطمینان حاصل شود که قابلیت اعتماد، تمامیت و در دسترس بودن دارایی‌های اطلاعاتی شرکت، در همه زمان‌ها، حفظ شده است [۲۰، صص۱۰-۱۴].

1. Armonk
2. Technikal Wave
3. Management Wave
4. Institutional Wave
5. Information Security Governance Wave

همانطور که ملاحظه می‌شود، در اینجا نیز، از موج اول به بعد، مباحث مدیریتی در امنیت اطلاعات نمایان‌تر شده‌است و براساس جدیدترین موج امنیت اطلاعات که به‌تازگی منتشر شده است، نقش مدیریت عالی، آموزش و آگاهی کاربر و خط مشی امنیتی به‌عنوان مبانی اصلی آن ذکر شده است.

به‌تازگی یک الگوی جدید در زمینه امنیت اطلاعات به‌وجود آمده است که به آن در مقام یک "*مسئلهٔ انسانی*" و یک "*مسئلهٔ سازمانی*" توجه می‌شود [۲۱، صص۲۷۱-۲۷۳]. امروزه به نظر می‌رسد، موفقیت امنیت اطلاعات تا حد زیادی به رفتار اثربخش کاربران وابسته است. رفتارهای درست و سازنده توسط کاربران، مدیران سیستم و افراد دیگر می‌تواند اثربخشی امنیت اطلاعات را تا حد زیادی بالا ببرد؛ در حالی که رفتارهای نادرست و مخرب، در حقیقت می‌تواند مانع اثربخشی آن شود.

پژوهش حاضر در راستای این الگوی جدید، رویکردی متفاوت از امنیت اطلاعات را با تمرکز بر "امنیت اطلاعات رفتاری[1]" ارائه می‌دهد. بنابراین با درنظرگرفتن فقدان یا کمبود عمومی تحقیق تجربی و اهمیّت امنیت اطلاعات برای سازمان‌های امروزی، این مطالعه در جست و جوی *شناسایی و مدلسازی سازه*[2]*های مدیریتی* حیاتی و اساسی‌ای است که بر اثربخشی امنیت اطلاعات در سازمان اثرگذار است. سازه‌های اساسی که در این پژوهش مورد بررسی قرار می‌گیرند عبارتند از:

- حمایت مدیریت عالی؛
- آموزش عوامل انسانی؛
- مهارت عوامل انسانی[3]؛
- تجربهٔ عوامل انسانی؛
- فرهنگ امنیتی؛
- تقویت خط‌مشی[4]؛
- اثربخشی امنیتی؛

---

1. Behavioral Information Security
2. Construct
3. Human Factor Sophistication
4. Policy Enforcement

• خودباوری افراد[1].

با توجه به بررسی مبانی نظری و پیشینهٔ پژوهش و بررسی تک تک این سازه‌ها و ارتباط آنها با امنیت سیستم‌های اطلاعاتی، جدول(۲) با عنوان مؤلفه‌ها و شاخص‌های هر یک از این سازه‌ها به‌صورت زیر تدوین شد:

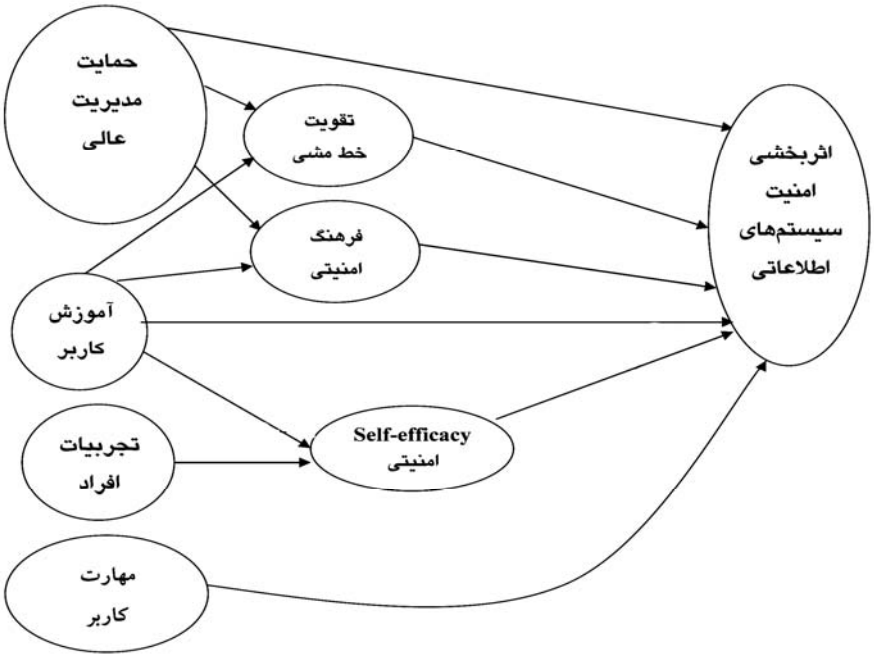
جدول۲ مؤلفه‌ها و شاخص‌های امنیت در این پژوهش (مستخرج از منابع پژوهش)

ردیف	مؤلفه	شاخصها	منبع
۱	اثربخشی امنیت سیستم‌های اطلاعاتی	حمایت مدیریت عالی فرهنگ امنیتی آموزش امنیتی خط‌مشی امنیتی تجربیات افراد خودباوری مهارت	٦-٢٢-٢٣-٢٥-٢٩-٣٢-٣٦-٤٢
۲	حمایت مدیریت عالی	درگیر شدن مدیر در فعالیت‌های ISS توافق شخصی بر خط‌مشی‌ها اولویت دادن به ISS	٦-٢٢-٢٨-٣٠
۳	فرهنگ امنیتی	نگرش سنت‌ها ارزش‌ها	٦-٢٤-٣٦
۴	آموزش امنیتی	برنامه‌های آموزش امنیتی ابزارهای آموزشی	٦-١٨-٣١-٣٣-٣٥
۵	خط مشی امنیتی	به‌روز بودن بازنگری کردن تعهد مدیریتی هم‌سویی با اهداف سازمان	٦-٢٧-٣٢-٤٤
۶	تجربیات (مستقیم و غیر مسقیم)	تخصص افراد توانایی‌های کامپیوتری زمان درگیر بودن در مباحث امنیتی	۲۵
۷	خود باوری	تجربیات آموزش قضاوت‌های شخصی	٢٥-٢٨-٣٩-٤٠
۸	مهارت	دانش، نیت	٤٢-٤٣

1. Self-efficacy

۴- روش شناسی پژوهش

در آغاز با استفاده از مطالعات کتابخانه‌ای و اکتشافی به‌بررسی مبانی نظری موضوع، و سپس شناسایی مؤلفه‌ها و شاخص‌های متغیرهای فرضیه‌ها پرداخته شده و با توجه به بررسی‌های انجام شده، مدل مفهومی پژوهش حاضر، در نمودار(۱) ارائه شده است.



نمودار۱ مدل مفهومی پژوهش

در راستای انجام این پژوهش فرضیه‌های زیر ارائه شد:

فرضیهٔ ۱. حمایت مدیریت عالی بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

فرضیهٔ ۲. حمایت مدیریت عالی از طریق فرهنگ امنیتی بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

فرضیهٔ ۳. حمایت مدیریت عالی از طریق تقویت خط مشی امنیتی بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

فرضیهٔ ٤. آموزش کاربر، بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

فرضیهٔ ٥. آموزش کاربر از طریق فرهنگ امنیتی، بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

فرضیهٔ ٦. آموزش کاربر از طریق خط‌مشی امنیتی، بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

فرضیهٔ ۷. آموزش کاربر از طریق خودباوری، بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

فرضیهٔ ۸. سطح مهارت عوامل انسانی، بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

فرضیهٔ ۹. تجربیات افراد (مستقیم یا غیر مستقیم) از طریق خودباوری افراد، بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر دارد.

برای نظرسنجی از خبرگان و به‌دست آوردن داده‌های اوّلیه (داده‌هایی که پیش از این وجود نداشته و باید توسط خود محقق ایجاد شوند) در راستای ارزیابی مدل پیشنهادی محقق، از روش‌های میدانی استفاده شده است. در روش‌های میدانی که از شهرت بیشتری برخودارند، روش پرسشنامه‌ای در گردآوری اطلاعات بسیار متداول است. در این پژوهش ابزار اصلی سنجش، پرسشنامه است. سوالات *با توجه به شاخص‌های به‌دست آمده از ادبیات تحقیق و نظریات استادان دانشگاهی*، برای سنجش *متغیرها* طراحی شده است.

جهت تعیین اعتبار و روایی پرسشنامه در این پژوهش، از روش اعتبار محتوا[1] استفاده شده است. برای تعیین روایی پرسشنامه نیز با مطالعه و ارزیابی دقیق پیشینهٔ موضوع، طرح اوّلیهٔ آن تهیه و توسط ده نفر از استادان و متخصصان بررسی شد و مواردی جهت اصلاح پیشنهاد و پس از اعمال اصلاحات مورد نظر، پرسشنامه نهایی تدوین گردید.

همچنین در این پژوهش برای تعیین پایایی پرسشنامه با استفاده از نرم‌افزار SPSS، مقدار ضریب آلفای کرونباخ پرسشنامه و که مقدار آن، برابر ۰٫۹۳۲ تعیین شد که چون

1. Content Validity

بزرگتر از ۰/۷۵ است، نشان می‌دهد که پرسشنامه از اعتبار کافی بهره‌مند است.

از آنجا که این پژوهش دربارهٔ "نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی" است، چند سازمانِ زیرمجموعهٔ وزارت ارتباطات و فناوری اطلاعات به‌عنوان جامعهٔ آماری انتخاب شدند. این سازمان‌ها عبارتند از: شرکت مخابرات، شرکت فناوری اطلاعات، شرکت ارتباطاتِ زیر ساخت و مرکز تحقیقات مخابرات ایران. همچنین برای نمونه‌گیری، از روش نمونه‌گیری خوشه‌ای به این صورت استفاده شده است که واحد فناوری اطلاعات هر یک از شرکت‌های جامعهٔ آماری به‌عنوان یک خوشه در نظر گرفته شده، سپس با مراجعه به این خوشه‌ها، از کارشناسان، خبرگان و مدیرانی که در زمینه IT فعالیت می‌کردند برای نظرسنجی انتخاب شدند. بدین ترتیب تعداد صد پرسشنامه بین کارشناسان، خبرگان و مدیران صاحب‌نظر سازمان‌های مذکور توزیع و از این تعداد ۸۸ پرسشنامه تکمیل شده جمع‌آوری شد که پس از حذف پرسشنامه‌های ناقص، داده‌های ۸۰ پرسشنامه مورد تجزیه و تحلیل قرار گرفت. از این میان سی و پنج نمونه مربوط به مرکز تحقیقات مخابرات ایران بود آن هم به این دلیل این که در این مرکز نسبت به سازمان‌های دیگر متخصصان بیشتری در زمینهٔ امنیت اطلاعات فعالیت می‌کنند و از سازمان‌های دیگر هر کدام پانزده نمونه انتخاب شد.

ابزار جمع‌آوری داده‌ها در این پژوهش پرسشنامه است. مقیاس اندازه‌گیریِ نگرشِ پاسخ دهنده در پرسشنامه، طیف لیکرت است. در این پرسشنامه هفت سطح متفاوت با هفت عبارت مشخص شده و رتبهٔ آنها به ترتیب از یک تا هفت در نظر گرفته شده است.

برای آزمون فرضیه‌ها با متغیرهای کیفی از آمار ناپارامتریک استفاده می‌شود. در این پژوهش، فنون تحلیل آماری در دو قسمت مورد استفاده قرار گرفته است:

۱. بررسی نظرات خبرگان در مورد وجود هر یک از متغیرهای پژوهش در سازمان.

۲. بررسی و آزمون فرضیه‌های تحقیق.

در آغاز برای تجزیه و تحلیل نظرات افراد، از *آزمون دو جمله‌ای*[1] استفاده شده‌است زیرا در ابزار جمع‌آوری اطلاعات از خبرگان خواسته شده است که در ارتباط با وجود یا عدم وجود نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی نظر خود را بیان کنند و این مطابق با شرایط آزمایش برنولی است که در آن موفقیت (p) به معنای تأیید آن عامل توسط خبره و

1. Binomial Test

شکست (q) به معنای ردّ آن است؛ بنابراین با توجه به این شرایط به بررسی وضعیت رد یا تأیید شدن متغیرها (سازه‌ها) پرداخته شد.

با توجه به این که هدف این پژوهش، تبیین مدلی برای بررسی نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی است و در آن تأثیر تعاملی چند متغیر بر روی یگدیگر بررسی می‌شود؛ بنابراین از نرم افزار LISREL استفاده شده است این نرم‌افزار یکی از مهمترین برنامه‌ها برای برآورد پارامترها، آزمون معناداری و برازش مدل‌های معادلات ساختاری با متغیرهای نهایی است که البّته غیر قابل مشاهده و اندازه‌گیری مستقیم هستند. لیزرل برای هریک از مسیرها ضریب مسیر و ارزش t را محاسبه می‌کند. ضریب مسیر تقریباً معادل ضریب رگرسیون می‌باشد و اگر مقدار ارزش t از ۲ بیشتر باشد، نشان دهندهٔ معنادار بودن مسیر است. آزمون فرضیه‌ها با توجه به ضرایب مسیر و مقدار t آن صورت می‌گیرد.

تجزیه وتحلیل داده‌ها و آزمون فرضیه‌ها

خلاصهٔ نظرات خبرگان در موردِ وجود یا عدم وجودِ هر یک از متغیرها به همراه نتایج آزمون دو جمله‌ای حاصل از نرم افزار آماری SPSS، به شرح جدول شمارهٔ ۳ می‌باشد. برای قضاوت در مورد تأیید یا رد هر یک از متغیرها به ستون سطح معناداری[1] توجه می‌شود، چنانچه مقدار این ستون کم‌تر از ۵٪ باشد، دلیل بر تأییدِ وجودِ نقش هر یک از عوامل انسانی در امنیت سیستم‌های اطلاعاتی است.

جدول۳ نتایج آزمون دوجمله‌ای در مورد نقش هر یک از عوامل انسانی در امنیت سیستم‌های اطلاعاتی

متغیرهای پژوهش	طبقه	فراوانی مشاهده شده	درصد مشاهدات	نسبت آزمون	سطح معناداری
حمایت مدیریت عالی	≤٤	۲۰	۰,۲۵	۰,۵۰	۰,۰۰۰
	>٤	٦۰	۰,۷٥		
آموزش کاربر	≤٤	۲۰	۰,۲٥	۰,۵۰	۰,۰۰۰
	>٤	٦۰	۰,۷٥		
فرهنگ امنیتی	≤٤	۲۳	۰,۲۹	۰,۵۰	۰,۰۰۰
	>٤	٥۷	۰,۷۱		

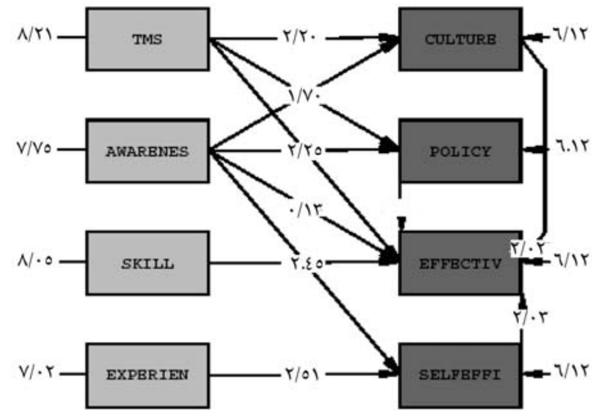
1. Asymp. Sig. (2-tailed)

ادامهٔ جدول۳

متغیرهای پژوهش	طبقه	فراوانی مشاهده شده	درصد مشاهدات	نسبت آزمون	سطح معناداری
مهارت کاربر	≤٤	۲۵	۰,۳۱	۰,۵۰	۰,۰۰۱
	>٤	۵۵	۰,٦۹		
تقویت خط مشی	≤٤	۲۰	۰,۲۵	۰,۵۰	۰,۰۰۰
	>٤	٦۰	۰,۷۵		
اثربخشی امنیتی	≤٤	۲٦	۰,۳۳	۰,۵۰	۰,۰۰۲
	>٤	۵٤	۰,٦۸		
تجربیات افراد	≤٤	۲۹	۰,۳٦	۰,۵۰	۰,۰۳۲
	>٤	۵۱	۰,٦٤		
خودباوری افراد	≤٤	۲٦	۰,۳۳	۰,۵۰	۰,۰۰۲
	>٤	۵٤	۰,٦۸		

همان طور که در جدول شمارهٔ ۳ ملاحظه می‌شود، از دیدگاه خبرگان مشارکت‌کننده در این پژوهش، حمایت مدیریت عالی، آموزش عوامل انسانی، مهارت عوامل انسانی، تجربهٔ عوامل انسانی، فرهنگ امنیتی، تقویت خط مشی، اثربخشی امنیتی، خودباوری افراد، در امنیت سیستم‌های اطلاعاتی نقش دارند.

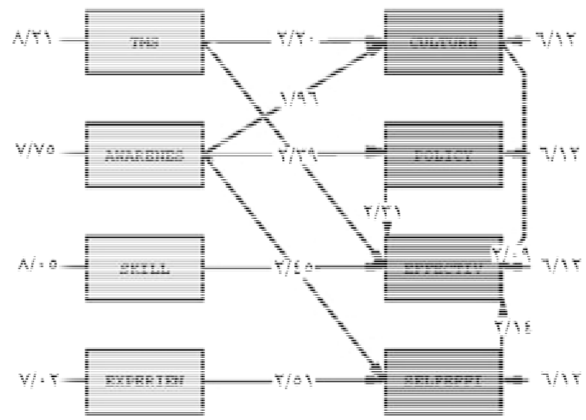
در ادامه برای آزمون تک تک فرضیه‌ها از نرم افزار LISREL (لیزرل) استفاده شد. نتایج انجام این آزمون همراه با مقادیر t-Value روابط، در نمودار (۲) نشان داده شده است. همان‌طور که در این نمودار مشاهده می‌شود؛ مقدارِ t ضریبِ مسیر مربوط به رابطهٔ متغیرهای «حمایت مدیریت عالی با تقویت خط‌مشی» و «آموزش کاربر با اثربخشی امنیتی» کم‌تر از ۲ می‌باشد، بنابراین فرضیه‌های ۳ و ٤ تأیید نشد اما بقیه فرضیه‌ها تأیید گردید.



Chi-Square= ۱۶/۰۸۴ , df= ۱۶ , P-value= ۰/۴۴۷۲۰ , RMSEA= ۰/۰۰۸۵

نمودار۲ نتایج حاصل از اجرای اولیه مدل توسط نرم افزار لیزرل

پس از حذف فرضیه‌های ردشده، نتایج نهایی به‌صورت مدل ارائه شده در نمودار ۳ حاصل گردید.



Chi-Square= ۱۸/۸٤ , df= ۱۸ , P-value= ۰/٤۰۱۵۲ , RMSEA= ۰/۰۲۵

نمودار۳ نتایج نهایی حاصل از نرم‌افزار ایزرل دربارهٔ نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی

پس از اینکه معناداری شاخه‌ها مورد بررسی قرار گرفت، این بار مجموعهٔ روابط متغیرها و کل مدل با استفاده از نرم‌افزار لیزرل مورد آزمون قرار گرفت تا معناداری مدل در کل مورد بررسی قرار گیرد. در لیزرل خوبی برازش مدل از طریق یک سری شاخص‌ها از جمله مقدار مربع کای، شاخص خوبیِ برازش (GFI)، شاخص خوبیِ برازش اصلاح شده (AGFI)، ارزش P (P-Value)، ریشهٔ میانگین مجذورات مانده و ریشه خطای مربع میانگین سنجیده شده است.

در این پژوهش، آزمون کای دو مجموعهٔ روابط علّی فوق با ۲۸ درجه آزادی برابر ۲۲۹,۲۵ می‌باشد و این نشان می‌دهد که در سطح ۹۵٪ روابط فوق معنادار است. همچنین مقدار GFI برابر ۰/۹۵ و مقدار AGFI برابر ۰/۸۳ است که چون مقدار هر دوی آنها بیشتر از ۰/۸۰ و نزدیک یک است؛ نشان از برازش خیلی خوب مدل دارد. مقدار خطا (RMSEA) نیز برابر ۰/۰۲۵ است.

Root Mean Square Residual (RMR) = ۰/۵۸

Standardized RMR ۰/۰۷۳

Goodness of Fit Index (GFI) ۰/۹۵

Adjusted Goodness of Fit Index (AGFI) = ۰/۸۳

Parsimony Goodness of Fit Index (PGFI) = ۰/۲٦

بنابراین در کل می‌توان گفت که برازش مدل خیلی خوب است و می‌توان گفت که مجموعه‌ای از متغیرهای "*حمایت مدیریت عالی*"،"*آموزش امنیتی*"، "*فرهنگ امنیتی*"، "*مهارت کاربر*"، "*خط مشی امنیتی*"، "*تجربیات افراد*" و "*خودباوری افراد*" به بهبود و بهینه شدن "*اثر بخشی امنیتی*" می‌انجامد.

۶- نتیجه‌گیری و پیشنهادها

هیچ سازمان یا سیستم اطلاعاتی‌ای وجود ندارد که بتواند امنیت را به‌صورت کامل برقرار کند یا ادعای داشتن آن را بکند. با وجود این، تمرین‌های خاصی وجود دارد که مدیران می‌توانند با استفاده از آن، حمایت و اثربخشی امنیتی‌شان را هر چه بیشتر تأمین کنند.

در ضمن پژوهش به این نتیجه رسیدیم که عوامل انسانی نسبت به عوامل فنی و تاکتیکی دارای تأثیر و ارزش بیشتری بر اثربخشی ISS هستند و بنابراین با توجه بیشتر به آنها، می‌توانیم تأثیر بیشتری بر روی بهبود اثربخشی امنیتی و حمایت از دارایی‌های اطلاعاتی در سازمان داشته باشیم. در این راستا با بررسی منابع پژوهش، بعضی از فاکتورهای مدیریتی و انسانی مؤثر بر اثربخشی ISS در سازمان‌ها شناسایی شدند و اثر هر یک از آنها بر اثربخشی مورد بررسی قرار گرفت.

همچنین معادلهٔ ساختاری تمامی متغیرهای نهایی به‌صورت زیر بیان می‌شود:

(خطا) ۷/۲۲ + (آموزش کاربر) *(۰/۲۳) + (حمایت مدیریت عالی) *(۰/۳۳)= فرهنگ امنیتی

(خطا) ٦/٥٧ + (آموزش کاربر) *(۰/۰٤۸) + (حمایت مدیریت عالی) *(۰/۲٤) = خط مشی

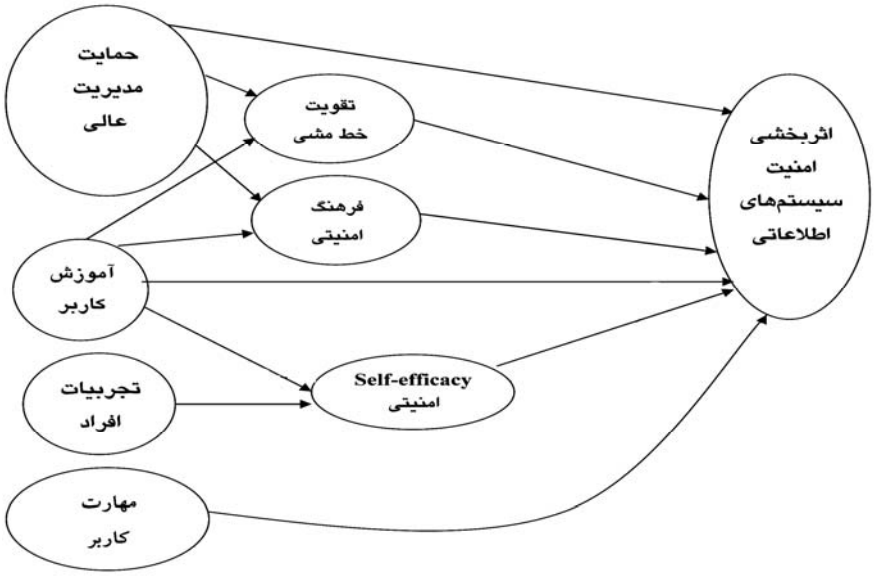
(خطا)۱۳/۱۷ + (تجربیات افراد) *(۰/۳۱) + (آموزش کاربر) * (۰/۳۷) = خودباوری افراد

(خودباوری افراد) *(۰/۱۷) + (خط مشی امنیتی)*(۰/۲۷)+(فرهنگ امنیتی)*(۰/۲۳) = اثربخشی امنیتی

(خطا) ۷/۱۹ + (مهارت کاربر)*(۰/٦۰) + (حمایت مدیریت عالی)*(۰/۳۷) +

بنابراین این معادلات می‌توانند به‌عنوان مبنایی برای اندازه گیری اثرات هر یک از این سازه (متغیر)های پژوهش بر اثربخشی امنیت سیستم‌های اطلاعاتی به کار روند.

در نهایت مدل زیر به‌عنوان مدل نهایی تحقیق حاضر ارائه شد:



نمودار۴ مدل نهایی پژوهش: مدل عوامل انسانی مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی

بر مبنای مرور منابع و اطلاعات دانشگاهی موجود در دنیا، مدل تئوریکی که در این پژوهش ارائه شد، مدلی است که سازه‌های مدیریتی و انسانی مرتبط با امنیت اطلاعات سازمانی را دربر می‌گیرد. مدل از لحاظ آماری به نتایج عمده‌ای دست یافته است که با یافته‌های کیفی اوّلیه (فرضیه‌های پژوهش) سازگار است.

به این دلیل که بسیاری از مسائل و مشکلات کامپیوتری و امنیتی، امروزه نیازمند راه‌حل‌های مدیریتی‌اند، مدل تئوریکی پیشنهاد شده در این مطالعه می‌تواند مدیران را کمک کند تا تلاشهای خود را بر نواحی‌ای متمرکز کنند که بتوانند بیش‌ترین تفاوت و اثربخشی را ایجاد کنند. مدیران می‌توانند با تفکر دربارهٔ مدل تئوریکی این پژوهش و به کارگیری آن برای سازمانهایشان، اثربخشی امنیت را بهبود بخشند. اگر چه این مدل همهٔ جنبه‌های مهم مدیریتی را شامل نمی‌شود، با این وجود مدل بر نواحی‌ای تمرکز کرده است که مدیران می‌توانند با نفوذ و اثرگذاری بر این نواحی، یک برنامه امنیت اطلاعات اثربخش بسازند.

در این پژوهش علاوه بر استفاده از متغیرهای مدیریتی به‌دست آمده از تحقیقات گذشته،

متغیرهای جدید دیگری نیز که بر اثربخشی امنیت سیستم‌های اطلاعاتی اثرگذارند از جمله فاکتور مهارت، به‌عنوان یکی از عوامل اثرگذار، شناسایی شده است. همچنین اثر آموزش امنیتی بر اثربخشی امنیتی، هم به‌صورت مستقیم و هم از طریق متغیرهای فرهنگ امنیتی، خط‌مشی امنیتی و خودباوری افراد و اثرات متغیرهای شناسایی شدهٔ قبلی در ارتباط با این متغیرها و در کل بر روی اثربخشی امنیتی بررسی و در نهایت یک مدل نهایی با عنوان "مدل عوامل انسانی مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی" ارائه شد.

بنابراین می‌توان گفت که در راستای شناسایی عوامل و فاکتورهای انسانی و مدیریتی اثرگذار بر امنیت ISS، مدل ارائه شدهٔ در این پژوهش، *یکی از کامل‌ترین مدل‌هایی* است که سازه‌های مدیریتی و انسانی اثرگذار بر اثربخشی ISS را دربرمی‌گیرد.

همچنین در راستای انجام تحقیقات بعدی، پیشنهادهای زیر به محققان آینده ارائه می‌شود:

۱. همان طور که بیان شد مدل ارائه شده در این پژوهش یکی از اوّلین و کامل‌ترین مدل‌هایی است که سازه‌های مدیریتی و انسانی مرتبط با امنیت سیستم‌های اطلاعاتی را در برگرفته است؛ امّا جامع نیست و آن همه سازه‌های مدیریتی مهم که ممکن است بر اثربخشی امنیتی مؤثر باشند را دربرنمی گیرد. سازه‌های دیگری نیز مانند مدیریت ریسک وجود دارد که بسیار مهم‌اند؛ امّا در این مدل جا داده نشده‌اند. بنابراین استفاده‌های آینده از این پژوهش و این مدل می‌تواند سازه‌های دیگری را به مدل اضافه کند.

۲. محققین امنیت اطلاعات می‌توانند مدل ارائه شده در این پژوهش را با به‌کارگیری نمونه‌های مختلفی از فرهنگ‌ها، صنایع یا رفرنس‌های مختلف دیگر مورد بررسی و آزمایش قرار دهند تا اثر آن در زمینه‌های مختلف بهتر شناسایی شود.

۳. بررسی‌هایی نیز در زمینهٔ امکان وجود ارتباط‌های دیگر، بین متغیرهای این پژوهش می‌توان انجام داد.

٤. بررسی علل بی‌توجهی به فاکتورهای مدیریتی و انسانی مؤثر بر امینت ISها.

٥. انجام مطالعات تطبیقی در زمینهٔ نقش عوامل انسانی در اثربخشی ISS، به منظور بهره‌گیری از تجربیات موفق سازمان‌ها و کشورهای موفق.

٦. بررسی راهکارهای بهبود اثر هر یک از فاکتورهای مدیریتی ارائه شده در این پژوهش بر اثربخشی امنیتی.

۷- منابع

[1] Schou, C.D. and K.J. Trimmer, Information Assurance and Security. *Journal of Organizational and End User Computing*, 16(3): p. i-vii, 2004.

[2] Bagchi, K. and G. Udo, An Analysis of the Growth of Computer and Internet Security Breaches. Communications of the AIS, 2003. 12(46): p. 684-700, 2004.

[3] Ammeter A, Douglas C, Gardner W, Hochwarter W, Ferris G. Toward a political theory of leadership. The Leadership Quarterly; 13:751e96, 2002.

[4] Computer Emergency Response Team (CERT), CERT Statistics. 2004.

[5] Gordon, L.A., et al., 9th Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute: San Francisco, CA, 2004.

[6] Kenneth J. Knapp, PhD, Thomas E. Marshall, PhD, R. Kelly Rainer, Jr., PhD. Nelson Ford, PhD, Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness, Management Information Systems Department College of Business ,Auburn University, Alabama, USA. October 25, 2005.

[7] Magklaras G, Furnell S. Insider threat prediction tool: evaluating the probability of IT misuse. Computers and Security; 21(1):62-73, 2002.

[8] Kathleen M. Carley, Information Security: The Human Perspective, Dept. of Social and Decision Sciences, Carnegie Mellon University, August 2000.

[9] Gary Hinson, IsecT Ltd, Human factors in information security, Innovative information security awareness programs, NoticeBored, 2003.

[10] Jose J Gonzalez, 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, 2002.

[11] Marianthi Theoharidou, Spyros Kokolakis, Maria Karyda, Evangelos Kiountouzis, The insider threat to information systems and the effectiveness of

ISO17799, Computers & Security, 24, 472-484, 2005.

[12] Gary Hinson, IsecT Ltd, Human factors in information security, Innovative information security awareness programs, NoticeBored, 2003.

[13] Kotulic, A.G. and J.G. Clark, Why There Aren't More Information Security Research Studies. Information & Management, 41(5): p. 597-607, 2004.

[14] Basie von Solmsa, Rossouw von Solms, From information security to business security?, Computers & Security, 24, 271-273, 2005.

[15] Jorma Kajava and Rauno Varonen, IT and the Human Body and Mind in the Information Security Perspective, European Intensive Programmeon Information and Communication Technologies Security, IPICS'2002, 3rd Winter School. Oulu, Finland. April 2-9, 2002.

[16] Bagchi, K. and G. Udo, An Analysis of the Growth of Computer and Internet Security Breaches. Communications of the AIS, 12(46): p. 684-700, 2003.

[17] Bento, A. and R. Bento, Empirical Test of a Hacking Model: An Exploratory Study. Communications of the AIS, 14(32): p. 678-690, 2004.

[18] Basie von Solmsa, Rossouw von Solms, The 10 deadly sins of information security management, Computers & Security, 23, 371-376, 2004.

[19] Basie von Solms, Information Security – The Fourth Wave, computers & security25, 165–168, 2006.

[20] PriceWaterhouseCoopers Internet portal. Information Security Breaches Survey 2004 e technical report.!http://www.pwc.com/images/gx/eng/about/svcs/grms/ 2004 Technical_Report.pdfO; 2004.

[21] Knapp, K.J., et al., Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC)2 Survey Results, Auburn University: Alabama 2004.

[22] Grover S. Kearns, The effect of top management support of SISP on strategic IS management: insights from the US electric power industry, Omega 34, 236 – 253, 2006.

[23] Bhanu S. Ragu-Nathana, Charles H. Apigianb, T.S. Ragu-Nathana, Qiang Tu, A path analytic study of the effect of top management support for information systems performance, Omega 32, 459 – 471, 2004.

[24] Cheryl Vroom, Rossouw von Solms, Towards information security behavioral compliance, Computers & Security, 23, 191-198, 2004.

[25] Danielc. Phelps, 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, 2005.

[26] E. von Solms and Prof J.H.P Eloff, Information Security Development Trends, Department Computer Science and Information Systems, University of South Africa, Pretoria, SA, 2004.

[27] Gritzalis D. A baseline security policy for distributed healthcare information systems. Computers and Security; 16(8): 709-19, 1997.

[28] Henderson JC, Venkatraman N. Strategic alignment: leveraging information technology for transforming organizations. *IBM Systems Journal*; 38(2,3):472–85, 1999.

[29] Kankanhalli, A., et al., An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*, 23(2): p. 139-154, 2003.

[30] Lederer AL, Mendelow AL. Convincing top management of the strategic potential of information systems. MIS Quarterly; 12(4):525–44, 1998.

[31] M.E. Thomson and R. von Solms, Information security awareness: educating your users effectively, Information Management & Computer Security 6/4, 167–173, 1998.

[32] Maria Karydaa, Evangelos Kiountouzisa, Spyros Kokolakis, Information systems security policies: a contextual perspective, Computers & Security , 24, 246-260., 2005.

[33] Mathisen, J. Measuring Information Security Awareness. Høgskolen i Gjøvik 2004.

[34] Organization for Economic Co-operation and Development (OECD), OECD Guidelines for the Security of Information Systems and Networks, 2002.

[35] Salanova, M., Grau, R. M., Cifre, E., & Llorens, S. Computer training, frequency of usage and burnout: the moderating role of computer self-efficacy. Computers in Human Behavior, 16, 575-590, 2000.

[36] 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), 2003.

[37] Schou, C.D. and K.J. Trimmer, Information Assurance and Security. Journal of Organizational and End User Computing, 16(3): pp. 123-145, 2004.

[38] Ajzen I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*; 32:665-83., 2002.

[39] Bandura, A. Self-Efficacy: Toward a Unifying Theory of Behavioral Change. Psychological Review, 84, 191-215, 1997.

[40] Bandura, A. Social Foundations of Thought and Action: A Social Cognitive Theory. Prentice-Hall, 1986.

[41] Bandura, A. Self-Efficacy. In V.S.Ramachaudran (Ed.), Encyclopedia of Human Behavior (pp. 71-81). New York: Academic Press., 1994.

[42] G.B. Magklaras, S.M. Furnell, A preliminary model of end user sophistication for insider threat prediction in IT systems Computers & Security, 24, 371-38., 2005.

[43] CNN.com. The case against Robert Hanssen. In-depth special series. http://edition.cnn.com/SPECIALS/hanssen, 2001.

[44] Trompeter C, Eloff J. A framework for the implementation of socio-ethical controls in information security. Computers and Security; 20(5):384-91, 2001.