فصلنامه

نظام ها و خدمات اطلاعاتی

سال اول، شماره ۲، بهار ۱۳۹۱، ص ص ۱-۱۶

ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران

دکتر محمد حسن زاده *

استادیار کتابداری و اطلاع رسانی، دانشگاه تربیت مدرس

دکتر داوود کریم‌زادگان مقدم

دکتری سیستم‌های گسسته، استادیار دانشکده فنی و مهندسی دانشگاه پیام‌نور

نرگس جهانگیری

هنرآموز کامپیوتر آموزش و پرورش، منطقه ۱۳

تاریخ دریافت: ۱۳۹۰/۸/۲۸ **تاریخ پذیرش:** ۱۳۹۰/۱۱/۱۷

چکیده

هدف: هدف از پژوهش حاضر ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران است. در این تحقیق، میزان سطح آگاهی از امنیت اطلاعات کاربران در سه سطح دانش، نگرش و رفتار مورد ارزیابی قرار گرفت.

روش: این تحقیق به لحاظ گردآوری اطلاعات به روش پیمایشی انجام گرفته است. برای محاسبه سطح آگاهی کارمندان از امنیت اطلاعات، ۷ مؤلفه بررسی شد. عوامل متنوعی که بر میزان آگاهی کاربران از امنیت اطلاعات به عنوان متغیر مستقل این تحقیق تأثیرگذار است، شناسایی شد که شامل متغیرهای مستقل جنسیت، میزان تحصیلات، میزان آشنایی با مهارت فنّاوری اطلاعات، میزان سابقه شغلی، درجه سازمانی، رشته تحصیلی و رده شغلی کارمندان بوده است.

یافته ها: پس از ارزیابی داده‌ها، اولویت و سطوح مؤلفه‌ها برای آموزش مشخص و اثبات شد که از بین ۷ متغیر مستقل، تنها آشنایی با مهارت فنّاوری اطلاعات، درجه سازمانی، رشته تحصیلی و رده شغلی کارمندان با پرمایگی آگاهی از امنیت اطلاعات آنان دارای همبستگی است.

نتیجه گیری: یافته های نشان می دهد که اولا آموزش امنیت اطلاعات ضرورت دارد، ثانیا، در برنامه ریزی آموزش امنیت اطلاعات به کارکنان بایستی درجه سازمانی، رشته تحصیلی و رده شغلی آنها مورد توجه قرار بگیرد تا آموزش ها بتواند موثر واقع شوند. اولویت هرکدام از مولفه ها در چارچوب نهایی مورد بحث قرار گرفته است.

کلیدواژه‌ها: آگاهی از امنیت اطلاعات، امنیت اطلاعات، پرمایگی، چارچوب مفهومی

*. نویسنده رابط hasanzadeh@modares.ac.ir

مقدّمه

در سال‌های اخیر با پیشرفت فنّاوری اطلاعات و ارتباطات، شاهد به‌کارگیری تجهیزات الکترونیکی و روش‌های مجازی در بخش عمده‌ای از فعالیت‌های روزمره همچون ارائه خدمات مدیریت و نظارت و اطلاع‌رسانی هستیم. فضایی که چنین فعالیت‌هایی در آن صورت می‌پذیرد، با عنوان فضای تبادل اطلاعات شناخته می‌شود. فضای مذکور همواره در معرض تهدیدهای الکترونیکی یا آسیب‌های فیزیکی از قبیل جرایم سازمان یافته به منظور ایجاد تغییر در محتوا یا جریان انتقال اطلاعات، تخریب بانک‌های اطلاعاتی، اختلال در ارائه خدمات اطلاع‌رسانی یا نظارتی و نقض حقوق مالکیت معنوی است.

از طرف دیگر با رشد و توسعه فزاینده فنّاوری اطلاعات[1] و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات افزایش یافته است و روش‌های اعمال تهدیدهای یادشده گسترده‌تر و پیچیده‌تر می‌شود. از این‌رو، حفظ ایمنی فضای تبادل اطلاعات از جمله مهم‌ترین اهداف توسعه فنّاوری اطلاعاتی و ارتباطی محسوب می‌شود (Wilson & Hash, 2003 ؛ Kruger & Kearrney, 2006 ؛ Veiga & Eloff, 2010).

یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقاء آگاهی کاربران از امنیت اطلاعات است. در این صورت، افراد آگاهی های لازم و مربوط به نقش و مسؤولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می کنند(Von Solms & Von Solms, 2004). آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و تقویت فعالیت‌های خوب امنیتی می‌شود و به افراد اجازه می‌دهد تا نسبت به امنیت فنّاوری اطلاعات نگران و پاسخ‌گو باشند (Wilson & Hash, 2003) و به تدریج به فرهنگ سازمان‌ها تبدیل خواهد شد (Kruger & Kearrney, 2006 ؛ Niekerk & Solms, 2009).

لذا بایستی به موازات تمهیدات فنی اعمال شده جهت امنیت اطلاعات، در قوانین و سیاست‌های جاری نیز متناسب با جایگاه نوین فضای تبادل اطلاعات در امور مدیریتی و اطلاع‌رسانی تجدید نظر شود و آموزش‌های صحیح به‌کارگیری اطلاعات و تأمین امنیت آنها با اولویت بالاتری در سطح جامعه ترویج شود. تحقیق حاضر به منظور ارائه یک چارچوب مفهومی برای این منظور انجام گرفته است.

فرضیه‌های پژوهش

۱. بین جنسیت کارکنان و پرمایگی آگاهی آنها از مؤلفه‌های امنیت اطلاعات، همبستگی وجود دارد.
۲. بین میزان تحصیلات کارکنان و پرمایگی آگاهی آنها از مؤلفه‌های امنیت اطلاعات، همبستگی وجود دارد.
۳. بین مهارت‌های فنّاوری اطلاعات کارکنان و پرمایگی آگاهی آنها از مؤلفه‌های امنیت اطلاعات، همبستگی وجود دارد.
۴. بین سابقه خدمت کارکنان و پرمایگی آگاهی آنها از مؤلفه‌های امنیت اطلاعات، همبستگی وجود دارد.
۵. بین درجه سازمانی کارکنان و پرمایگی آگاهی آنها از مؤلفه‌های امنیت اطلاعات، همبستگی وجود دارد.
۶. بین رشته تحصیلی کارکنان و پرمایگی آگاهی آنها از مؤلفه‌های امنیت اطلاعات، همبستگی وجود دارد.
۷. بین رده شغلی کارکنان و پرمایگی آگاهی آنها از مؤلفه‌های امنیت اطلاعات، همبستگی وجود دارد.

چارچوب نظری پژوهش

قبل از ظهور عصر شبکه‌ها، اطلاعات به صورت پرونده‌های کاغذی بایگانی می‌شد. اگر چه این رویه هنوز رایج است، با پدید آمدن شبکه‌ها و دسترسی آسان به اینترنت، قسمت اعظم اطلاعات از طریق این بستر در حال انتقال و پردازش است. بیشتر اطلاعات

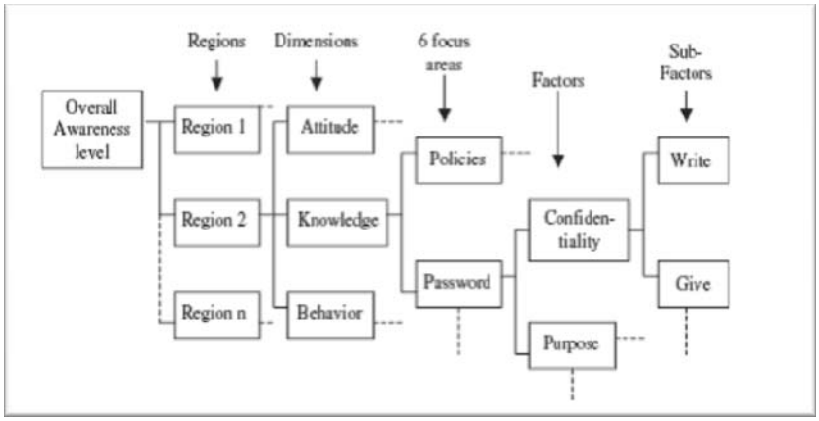
1. Information Technology

به صورت دیجیتالی ذخیره و بازیابی شده و با سرعت و دقت بالاتری در حال انتشار و تکثیر است. به موازات گسترش شبکه‌های محلی و سراسری، تهدیدات و سرقت و تخریب اطلاعات نیز افزایش یافته به طوری که شاید یکی از مهم‌ترین مسائل در عصر اطلاعات، حفاظت و امنیت آنهاست.

از اواخر دهه ۱۹۸۰ به بعد، استانداردهای مختلفی برای امنیت اطلاعات همچون، ISO/IEC , ISO/IEC 27001 S7799 TR13335, ایجاد شد و خیلی از سازمانها با پیاده سازی سیستم‌های مدیریت امنیت اطلاعات (ISMS) برای ارزیابی امنیت سیستم‌های اطلاعاتی تا حدودی امنیت اطلاعات را برای خود تأمین کردند (شیرازی و آل‌شیخ ، ۱۳۸۹، ص ۸۹). از سال ۲۰۰۰ تاکنون تحقیقات متعددی در ارتباط با ارزیابی آگاهی از امنیت اطلاعات انجام شده که در ادامه ارائه شده است.

ماکوناچی[1] و دیگران (Maconacchy, et al., 2001) ابعاد مهم در امنیت اطلاعات را بررسی کرده‌اند. توجه به مشخصات اصلی امنیت اطلاعات (در دسترس بودن، صحت، قابلیت اعتماد) و اقدامات امنیتی (فنّاوری، سیاست‌ها، رویه‌ها و آموزش و آگاهی) و وضعیت‌های اطلاعات (وضعیت انتقال و حافظه‌ها و پردازش) در رسیدن به امنیت اطلاعات مورد بررسی قرار گرفت.

کراگر و کرنی (Kruger & Kearrney, 2006) در تحقیقی در زمینه ارزیابی میزان آگاهی کارکنان از امنیت اطلاعات در شرکت‌های بین‌المللی معادن، نتایج مهمی در موارد مختلف امنیتی به دست آوردند. آنها سطوح آگاهی از امنیت اطلاعات را در سه سطح دانش، نگرش و رفتار تقسیم کردند و نواحی مورد ارزیابی در این سه سطح، شامل پایبندی به سیاست‌ها، ایجاد و نگهداری رمزهای مطمئن، بحث اینترنت و ایمیل، ایمنی تجهیزات سیار در انتقال اطلاعات، گزارش دهی وقایع امنیتی و عمل و عکس‌العمل مناسب بود.

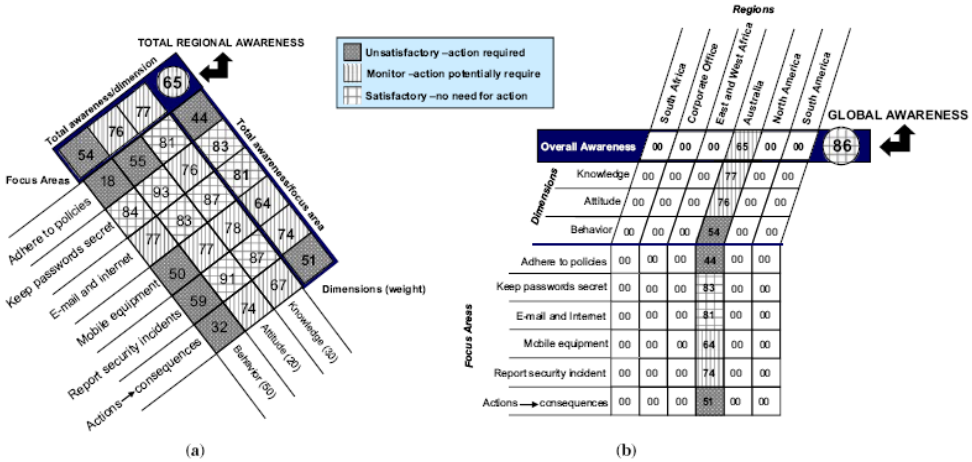


شکل ۱. مدل ارزیابی آگاهی از امنیت اطلاعات کاربران (Kruger & Kearrney, 2006)

این پژوهشگران پس از ارزیابی های خود به این نتیجه رسیدند که در کل، سطح آگاهی کارمندان از امنیت اطلاعات در حد متوسطی (۶۵) قرار دارد و به آموزش و توجه بیشتری نیاز است و برای بالا بردن سطح آگاهی از امنیت اطلاعات لازم است در هرکدام از حیطه های دانش، نگرش تلاش بیشتری انجام دهند.

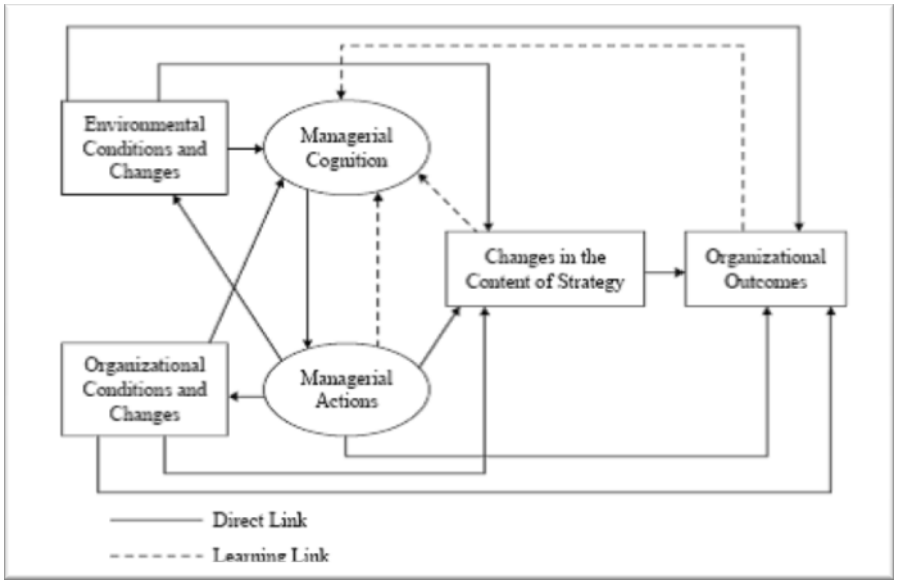
در پژوهش دیگری توسط چانگ (Chang, 2007) نیز نتیجه گرفته شد که فرهنگ سازمانی، تأثیر مستقیم بر ایجاد فرهنگ امنیت اطلاعات دارد. از جمله مؤلفه‌های سازمانی شامل همکاری، نوآوری، سازگاری، کارایی و تأثیربخشی بر روی اصول امنیت اطلاعات (محرمانگی، در دسترس بودن، صحت و پاسخگویی) بررسی شد و یافته ها نشان داد که تمام عوامل فرهنگ سازمانی بر مؤلفه‌های امنیت اطلاعات تأثیر مثبتی دارد.

1. Maconacchy



شکل ۲. (a) نقشه ارزیابی از آگاهی امنیت اطلاعات در استرالیا و (b) آگاهی در صورت کلی (Kruger and Kearrney, 2006)

در یکی از تحقیقات مهم در این زمینه که توسط چو ، کیم و جو (Choi et al., 2008) انجام شد، یافته‌ها حاکی از آن بود که افزایش میزان مدیریت آگاهی و دانش کاربران از امنیت اطلاعات تأثیری مستقیم بر نحوه مدیریت عمل و رفتار امنیتی کارکنان خواهد گذاشت و در نتیجه، عملکرد سازمان بهبود خواهد یافت.



شکل ۳: تأثیر مستقیم آگاهی از امنیت اطلاعات بر عملکرد سازمان (Choi, Kim, Dan & Goo, 2008)

در تحقیق دیگری با عنوان «مدلی برای آگاهی و بازیابی امنیت اطلاعات» که توسط اسمیت و کریتزینگر (Kritzinger & Smith, 2008) انجام شد، نمای کلی برای مدیریت امنیت اطلاعات (مستخرج از اسناد امنیت اطلاعات همچون استانداردها، گزارش‌ها و NIST و غیره) به دو قسمت موضوعات فنی و غیر فنی تقسیم شد، که از جمله موضوعات غیر فنی تأثیرگذار برای مدیریت امنیت اطلاعات، موضوع عوامل انسانی بود.

یکی دیگر از تحقیقاتی که مستقیماً به موضوع آگاهی از امنیت اطلاعات می‌پردازد، مربوط به شاو و دیگران (Shaw, Charlie, Harris, & Huang, 2009) با عنوان «بررسی ارزیابی غنای اطلاعاتی بر آگاهی از امنیت اطلاعات کاربران در

محیط آن‌لاین» است. آنها آگاهی از امنیت اطلاعات را به سه سطح دریافت[1]، درک[2] و برون‌دهی (که متناسب با تحقیق کراگر بود) تقسیم و میزان غنای اطلاعات در آموزش آن‌لاین را بر اساس ابرمتن[3]، چندرسانه‌ای[4] و ابررسانه‌ای[5] افراز کردند و از طریق آموزش الکترونیکی در یک محیط عینی حدود ۲۵۰ دانشجو رشته مدیریت سیستم‌های اطلاعاتی[6] را مورد بررسی قرار دادند. آنها به این نتیجه رسیدند که بین این سطوح رابطه مثبت برقرار است به طوری که فرد با دریافت بیشتر در سطح بالاتری از درک قرار می گیرد و با درک بیشتر در رفتار نیز موفقیت بیشتری کسب می کند. همچنین برای رسیدن به سطوح بالاتر آگاهی از امنیت اطلاعات که همان برون‌دهی و رفتار است، هر چه غنای اطلاعاتی بیشتر باشد سطح آگاهی از امنیت اطلاعات نیز بالاتر می‌رود، به طوری که تأثیر آموزش ابررسانه‌ای تأثیر بیشتری نسبت به چندرسانه‌ای و ابرمتن دارد.

تحقیقی دیگر با عنوان شکل‌گیری فرهنگ امنیت اطلاعات در سازمان و تفاوت آن با فرهنگ سازمانی توسط سلمز و نیکرک (Nikrerk & Solms, 2009) ارائه شد؛ و به این نتیجه رسید که در ایجاد فرهنگ امنیت اطلاعات علاوه بر مصنوعات و ارزش‌های پذیرفته شده و احساسات و اعتقادات کارمندان، دانش و آگاهی کارمندان از امنیت اطلاعات تأثیر بسزایی دارد.

در تحقیقی دیگر، که توسط ویگا و الوف (Veiga & Eloff, 2010) انجام گرفت، چارچوبی برای ایجاد فرهنگ امنیت اطلاعات ارائه شد. وی تبیین مدل خود را بدین صورت بیان نمود که برخی از مؤلفه‌ها مانند رهبری و حاکمیت در سازمان، تغییر، سیاست‌های امنیتی، رویه‌ها و عملیات با تأثیرگذاری بر رفتار چه به صورت فردی، گروهی و سازمانی منجر به ایجاد فرهنگ امنیت اطلاعات در سازمان خواهند شد.

تحقیق دیگری توسط کراگر و کرنی (Kruger, Drevin & Steyn, 2010) با عنوان «ارزیابی آگاهی از امنیت اطلاعات از طریق یک آزمون در سطح دانش و رفتار کاربران» صورت گرفت. آنها به این نتیجه رسیدند که افزایش میزان سطح آگاهی از امنیت اطلاعات کارمندان از طریق آزمون لغات و مفاهیم، بسیار مفید است و رابطه مشخصی بین یادگیری امنیت اطلاعات و تغییر در رفتار امنیتی کاربران وجود دارد.

در تحقیقات داخلی مهم‌ترین پژوهش که در زمینه عوامل انسانی مؤثر در امنیت اطلاعات صورت گرفته، پژوهش طاهری (۱۳۸۶) با عنوان «ارائه یک چارچوب برای نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی» است. در این چارچوب عواملی همچون حمایت مدیر ارشد، خودباوری، مهارت کاربر، تجربه، فرهنگ و آموزش بر امنیت سیستم‌های اطلاعاتی مورد تأیید قرار گرفت. همان‌طور که مشهود است یکی از عامل تأثیرگذار بر امنیت اطلاعات، موضوع آگاهی و آموزش کاربران است.

با توجه به پیشینه ارائه شده، موضوع آگاهی از امنیت اطلاعات یکی از عوامل غیر فنی و انسانی مؤثر در امنیت اطلاعات در سازمان است که نسبت به راه‌حل‌های فنی، کمتر به آن توجه شده است. این در حالی است که این عامل می‌تواند سبب کارایی بالاتر سازمان در عصر اطلاعات باشد. در هر سازمان مسؤولین ذی‌ربط می توانند با توجه بیشتر و برنامه‌ریزی صحیح در این زمینه، سبب نهادینه شدن رفتارهای خوب امنیتی در کارمندان و فرهنگ امنیت اطلاعات در سازمان شوند و در پیاده‌سازی امنیت اطلاعات به موفقیت بیشتر نائل آیند. بنا به نظر طاهری (۱۳۸۶، ص ۵۷)، سازمان‌ها و مؤسسات تجاری با پیاده‌سازی یک استراتژی امنیت اطلاعات از مزایای زیر بهره‌مند خواهند شد:

کاهش احتمال غیرفعال شدن سیستم‌ها و برنامه‌ها (از دست دادن فرصت‌ها)

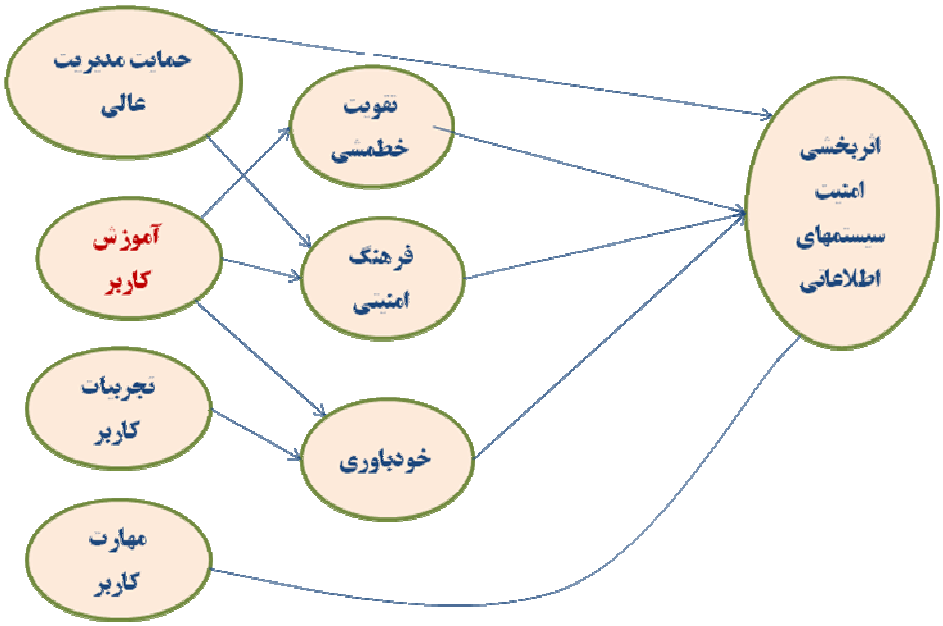
1. Perception
2. Comprehension
3. Hypertext
4. Multimedia
5. Hyper media
6. MIS

استفاده مؤثر از منابع انسانی[1] و غیرانسانی در یک سازمان (افزایش بهره‌وری)

کاهش هزینه از دست دادن داده‌ها و اطلاعات توسط ویروس[2]های مخرب و یا حفره‌های امنیتی[3] (حفاظت از داده‌های ارزشمند)

ارتقای حفاظت از مالکیت معنوی[4]

هزینه پیشگیری از یک مشکل امنیتی، همواره کمتر از هزینه بازسازی خرابی متأثر از آن است.



شکل ٤. مدل عوامل انسانی اثر گذار بر اثربخشی امنیت سیستم‌های اطلاعاتی (طاهری،١٣٨٦)

نقش عوامل انسانی در امنیت اطلاعات

ون و ماریوس (۲۰۰۴؛ نقل در طاهری، ۱۳۸۶) امنیت اطلاعات را به سه جنبه تقسیم بندی کرده‌اند:

شکل ٥ : جنبه‌های مختلف در امنیت اطلاعات

1. Human Resources
2. Virus
3. Security holes
4. Intellectual property

کنترل های دست‌یابی فیزیکی و سیستم‌های فنّاوری اطلاعات مثال‌هایی از بعد فنّاوری هستند که حمایت‌هایی برای دیگران فراهم می‌کنند. این سیستم‌ها معمولاً خدماتی فراهم می‌کنند که برای به‌کارگیری کنترل‌های دست‌یابی حیاتی‌هستند. فرایندهای امنیتی نشان می‌دهد که چگونه شرکتها به صورت رسمی و غیر رسمی عمل می‌کند. این قدرت نمایش، فراگیر است و همه خط‌مشی‌ها فعالیت‌های روتین رویه‌ها و رهنمودها و همچنین تعامل با مشتریان، عرضه‌کنندگان و شرکای تجاری و حتی برنامه‌های اقتضایی برای کشف هر موقعیت بحرانی را در بر می‌گیرد. در نهایت عامل انسانی توصیف می‌کند که چگونه افراد همگام با سیستم‌ها و فرایندهای سازمانی تکامل می‌یابند. البته، معمولاً به عامل انسانی کمتر توجه می شود؛ شاید به این خاطر که مانند جنبه‌های دیگر، کمیت‌پذیر و قابل سنجش نیست (طاهری، ۱۳۸۶، ص ۲۵).

در مطالعه ای که در سال ۲۰۰۵ توسط کمیسیون نظارتی در انگلستان درباره استفاده‌های نادرست از فنّاوری اطلاعات انجام شد ، مشخص شد که بیشتر دلایل استفاده نادرست به فاکتورهای مرتبط به افراد بر می‌گردد (کمیسیون بررسی[1]، ۲۰۰۵ به نقل از طاهری، ۱۳۸۶). در برنامه‌های امنیت سیستم‌های اطلاعاتی، افراد اغلب به عنوان ضعیف‌ترین عامل محسوب می‌شوند (Kruger & Kearrney, 2006). به طوری که گری هینسون (Gary hinson, 2003) راه‌حل فنی بالاتر از حد نیاز را برای سازمان مضر می‌داند. حتی در صورت ایجاد کلیه تمهیدات فنی و سیاست‌های امنیتی، عدم آگاهی و بی‌توجهی کاربران می‌تواند تمامی حفاظت‌های فنی را بی‌نتیجه سازد (Kruger & Kearney, 2006). در صورتی که کاربران آگاه در محیط کاری تا اندازه زیادی موجب کاهش این خطرات امنیتی می‌شوند (Wilson & Hash, 2003) و ارتقا دادن رفتارهای خوب کاربر و مقابله با رفتارهای بد، بستر مناسبی برای ارتقای اثربخشی امنیت اطلاعات در درون سازمان فراهم می‌کند (Stanton, Stam, Mastrangelo, and Jolton, 2005). گزارش ENISA در سال ۲۰۰۸ نشان داده که ۴۷٪ حوادث امنیتی به خاطر اشتباهات انسانی صورت گرفته است(طاهری، ص ۵۶، ۱۳۸۶).

به مقوله امنیت اطلاعات در عصر اطلاعات نه به صورت یک کالا و یا محصول، بلکه به صورت یک فرآیند سازمانی باید نگریست (Crowston & Williams, 2000) و امنیت در حد یک محصول خواه نرم‌افزاری و یا سخت‌افزاری تنزل داده نشود. هر یک از موارد فوق، جایگاه خاص با وزن مشخص شده‌ای دارند و نباید به بهانه پرداختن به امنیت اطلاعات، وزن یک پارامتر بیش از آن چیزی که هست در نظر گرفته شود و پارامتر دیگری نادیده انگاشته و یا وزن غیر قابل قبولی برای آن مشخص شود. به هر حال ظهور و عرضه شگفت‌انگیز فنّاوری‌های نو در عصر حاضر، تهدیدات خاص خود را نیز به دنبال خواهد داشت. ما چه می‌بایست انجام دهیم که از فنّاوری‌ها استفاده مفیدی داشته باشیم و در عین حال از تهدیدات مستقیم و یا غیر مستقیم آن مصون بمانیم؟ قطعاً نقش عوامل انسانی که استفاده‌کنندگان مستقیم این نوع فنّاوری‌ها هستند، بسیار مهم است.

آگاهی و آموزش امنیت اطلاعات به کاربران

همان طور که بیان شد یکی از جنبه‌های مهم در مدیریت امنیت اطلاعات در سازمان، توجه به امنیت ازمنظرمنابع انسانی است، به طوری که بدون در نظر گرفتن عوامل انسانی راه‌حل‌های فنی چندان تأثیری در مدیریت امنیت اطلاعات نخواهند داشت (Kruger & Kearrney, 2006). از جمله فاکتورهای مؤثر عوامل انسانی در تأمین امنیت اطلاعات، موضوع آگاهی و آموزش امنیت اطلاعات کاربران است (Wood, 1995؛ Thomson & Von Solms,1998؛ Wilson & Hash, 2003؛ Kruger & Kearrney, 2006؛ Shaw et al., 2009).

به طور کلی، یک ساختار تأثیرگذار امنیتی باید ترکیبی از عناصر تکنیکی و کاربردی باشد تا تأثیری متقابل بر روی خطرات ناشی از اطلاعات قابل حذف داشته باشد. با سریع‌تر شدن آهنگ تغییرات فنّاوری، نیاز به تدابیر منعطف امنیتی نیز بیشتر احساس

1. Audit Commission

می‌شود؛ لذا اداره صحیح اطلاعات قابل حذف و آگاه‌سازی تمامی کارکنان از این خطمشی، چاره‌اندیشی‌ها و روش‌های استفاده از آن، باید بخشی از سیاست‌های امنیتی باشد و با سیاست‌گذاری‌های مناسب همره باشد. کارکنانی که با اطلاعات حیاتی سر و کار دارند باید از مفهوم امنیت اطلاعات قابل حذف، آگاهی کامل پیدا کنند. اگر آگاهی و آموزش امنیتی به عنوان بخشی از مشاغل در نظر گرفته شود، افراد نسبت به شغل و وظیفه خود احساس مسؤولیت می‌کنند (Thomson, & Von Solms,1998؛ Kruger & Kearrney, 2006 ؛Wilson & Hash, 2003).

درباره بحث آموزش، تربیت و آگاهی نیروی انسانی بحث‌های زیادی انجام شده است. دلیل آن این است که آنها اساساً یک مسأله مرتبط با عوامل انسانی هستند. این مهم است که تشخیص دهیم که مسائل انسانی در بیشتر مواقع علت اصلی نواقص امنیتی است. یکی از بهترین راه‌های کاهش ریسک‌های امنیت اطلاعات در سازمان‌ها، آگاه‌سازی هر چه بیشتر کارمندان نسبت به مسائل امنیتی است. این آگاهی به این معناست که آنها باید مسؤولیت اعمال خود در محیط کاری را به عهده بگیرند (Solms & Solms, 2004).

در یک بررسی که در سال ۲۰۰۲ درباره استفاده نادرست از فنّاوری اطلاعات، توسط کمیسیون نظارت انگلستان انجام شد، بیان شد که اکثر دلایل این استفاده‌های نادرست به افراد مربوط می‌شود. از این میان یک سوم موارد گزارش شده مربوط به فقدان آگاهی امنیتی و ۲۳٪ هم ناشی از عدم آموزش کافی یا نادرست بود. این نشان می‌دهد اگر افراد می‌خواهند امنیت اطلاعات را به صورت اثربخشی تأمین کنند، نیاز است آنچه را که از آنها انتظار می‌رود، بهتر بدانند. همچنین بنا بر نتایج گزارش، موضوع آگاهی‌رسانی و آموزش کاربران از مسائل امنیتی بعد از مسأله حمایت توسط مدیریت، از مهم‌ترین مباحث امنیتی است (Kruger & Kearney, 2006).

طیف دانش امنیت اطلاعات کاربران

طبق تعریف NIST،[1] مراحل ارتقای دانش امنیت اطلاعات کاربران به سطوح زیر تقسیم می‌شود:

۱. آگاهی[2]
۲. تربیت[3]
۳. تحصیلات و آموزش[4]

یادگیری دانش امنیت اطلاعات در سطح پایین که مربوط به همه کاربران می‌شود، از آگاهی (موضوع مورد تحقیق) شروع می‌شود و با آشنایی با مفاهیم و ادبیات امنیت وارد مرحله تربیت می‌شود که مختص مسؤولین امنیت اطلاعات است. سپس با آموزش‌های ویژه که مخصوص افراد متخصص در زمینه امنیت اطلاعات است وارد مرحله آموزش و تخصص می‌شود.

آگاهی

آگاهی، صرفاً آموزش نیست و هدف از آگاهی تمرکز بر اهمّیت امنیت است. توجه به مقوله آگاهی به افراد اجازه می‌دهد تا نگرانی‌ها و مسؤولیت‌های امنیت فنّاوری اطلاعات را تشخیص دهند. آگاهی‌رسانی امنیتی، مختص تمامی کارمندان سازمان است. هدف آگاهی‌رسانی امنیتی، به صورت ساده، جلب توجه مخاطبین به اهمیت مقوله امنیت در سطح سازمان و ایجاد هوشیاری امنیتی بیشتر در بین مخاطبین است. به طوری که کارمند به سادگی از کنار مسائل به ظاهر جزئی نگذرند و به موقع نگرانی‌های امنیتی را

1. National Instituteof Standards and Technology
2. Awareness
3. Training
4. Education

تشخیص داده، عملکرد مناسبی در سطح وظایف و اختیارات خود انجام دهند. ابزارهای مناسب برای این امر عبارتند از: پوستر، بولتن، روزنامه، آموزش آنلاین و آموزش‌های مبتنی بر شبکه.

سطوح آگاهی از امنیت اطلاعات

رفتار امنیتی ضعیف برخی از کاربران (مثلاً خطاهای امنیتی کاربران، بی دقتی و عدم توجه) در بسیاری از رخدادهای امنیتی دخیل بوده است (Wilson & Hash, 2003؛ Kruger & Kearrney, 2006). بسیاری از سازمان‌ها به اهمیت برقراری یک برنامه برای آگاهی‌رسانی پیرامون امنیت اطلاعاتی در سازمان‌های خود پی برده‌اند (Wilson & Hash, 2003؛ Shaw et al., 2009). در موفقیت این نوع برنامه‌ها، حصول اطمینان از اینکه کارمندان به سه سطح از آگاهی از خطرات امنیتی می‌رسند بسیار دخیل است که این سه سطح متناسب با تحقیقات انجام شده، عبارتند از: دانش، درک و نگرش و رفتار و برون دهی (Kruger & Kearrney, 2006).

با پیشرفت کارمندان یک سازمان در راستای این سه سطح، امنیت از سوی افراد بالاتر می‌رود. بالا رفتن آگاهی امنیتی افراد و کاربران نهایی می‌تواند به تغییر فرهنگ‌ها و ارزش‌های امنیتی کمک کند و از این طریق صلاحیت امنیتی بهتری ایجاد می‌شود. اگرچه روشی واحد برای برنامه‌های مربوط به آگاهی امنیتی که با تمامی موقعیت‌ها در سطح سازمانی و انسانی در عملکردهای مختلف وجود ندارد، داشتن یک روش ثابت برای برقراری یک برنامه‌ی آگاهی امنیتی بر اساس سطوح آگاهی امنیتی بسیار ضروری است.

سطح اول آگاهی امنیتی: دانش

اولین گام در تأمین امنیت یک سازمان، آگاهی یافتن و کسب دانش و اطلاعات لازم جهت درک خطرات امنیتی محیط شغلی است. دانش یعنی شناسایی حضور یک تهدید و آگاه شدن از آن با توجه به اطلاعات قبلی. مزایای تشکیل یک تصویر صحیح از تهدیدات امنیتی محیط اطراف تا حد زیادی می‌تواند با ارتقای مشاهده و درک آگاهی امنیتی تقویت شود (Kruger & Kearrney, 2006).

سطح دوم آگاهی امنیتی: نگرش

داشتن دانش و اطلاعات کافی از نحوه رخداد حوادث امنیتی و تأثیرات آن به تنهایی کارساز نیست، بلکه کاربران باید به این حد از فهم برسند که امنیت اطلاعات و رعایت نکات ایمنی به هنگام استفاده از اطلاعات و فنّاوری اطلاعات، در مرحله اول به نفع خود آنها و سپس سازمان آنهاست. لذا با داشتن یک نگرش مثبت می‌توانند از دانش خود (سطح اول) به بهترین شکل استفاده کرده، حتی آن‌را بنا به نیاز ارتقا دهند (Kruger & Kearrney, 2006).

سطح سوم آگاهی امنیتی: رفتار و برون دهی

پیشگیری بهتر از درمان است. برای اجتناب از بروز خطرات امنیتی، کاربران نهایی باید توانایی برون دهی یا پیش‌بینی دوره‌های بعدی حملات امنیتی را داشته باشند. برون‌دهی، سومین سطح از ارتقای آگاهی امنیتی است. در این سطح رفتارها و عادت‌های خوب امنیتی در فرد ایجاد می‌شود و به ساختن فرهنگ امنیت اطلاعاتی منجر می‌شود. تصمیمات به موقع را می‌توان با آمادگی در توانایی برون‌دهی و رفتار گرفت. هدف غایی یک برنامهٔ کارآمد آگاهی امنیتی، آماده سازی کاربران با توانایی برون‌دهی خطرات امنیتی بالقوه است (Kruger & Kearrney, 2006).

آگاهی از امنیت اطلاعات در کاربران چه مؤلفه‌هایی را شامل می‌شود؟

در این تحقیق با بررسی محیط عینی سازمان و مشاوره افراد خبره در این زمینه، ۹ مؤلفهٔ زیر در جهت ارزیابی سطح آگاهی از امنیت اطلاعات مورد استفاده قرار گرفت:

ایمیل، ضمایم[1] و اسپم (هرزنامه)[2]

پشتیبانی

رمز عبور

بدافزارها[3](ویروس و کرم و تراجان‌ها و ...)

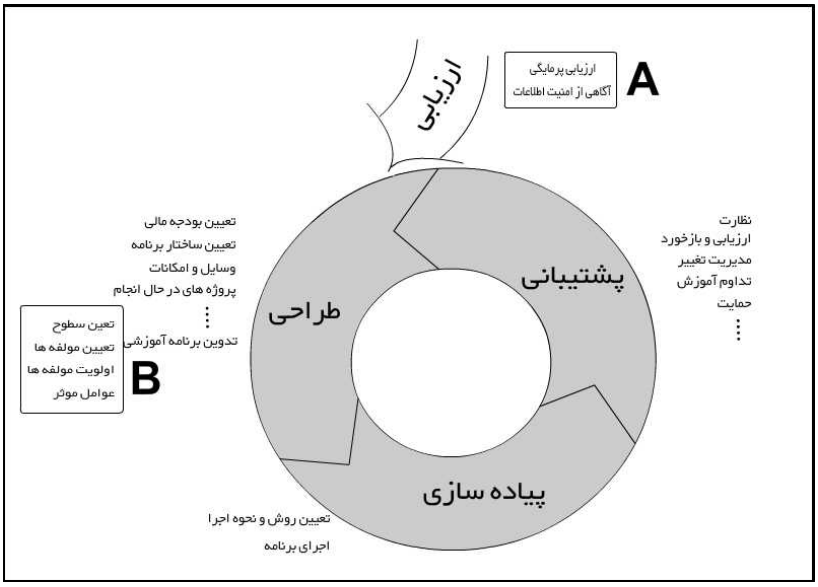
انتقال ایمن اطلاعات[4]

مهندسی اجتماعی[5]

گزارش‌دهی[6] حوادث امنیتی

التزام و رعایت سیاست‌های امنیتی[7] سازمان

چارچوب کلی ارتقاء آگاهی از امنیت اطلاعات کاربران در شکل زیر آمده است.



شکل ۳ : چارچوب کلی ارتقاء آگاهی از امنیت اطلاعات کاربران

روش‌شناسی

تحقیق حاضر به لحاظ هدف، از نوع کاربردی و از نظر روش گردآوری اطلاعات از نوع پیمایشی است. در این تحقیق متغیر وابسته، میزان آگاهی از امنیت اطلاعات کارمندان است که بر اساس ادبیات تحقیق و نظر خبرگان در نه مؤلفه ایمیل، ضمایم و

1. attachment
2. spam
3. Malware
4. Mobile Security
5. social engineer
6. Reporting
7. Adhere to policy

هرزنامه، پشتیبانی، رمز عبور، ایمنی در اینترنت، بدافزارها (ویروس و کرم و تراجان‌ها و ...)، انتقال ایمن اطلاعات، مهندسی اجتماعی، گزارش دهی حوادث امنیتی، التزام و رعایت سیاست‌های امنیتی سازمان، در سه سطح دانش، نگرش و رفتار محاسبه می‌شود. سپس ارتباط و میزان متغیر وابسته با متغیرهای مستقل مورد سنجش قرار می‌گیرد. متغیرهای مستقل شامل ۷ متغیر جنسیت، سابقه کاری، میزان تحصیلات، آشنایی با مهارت‌های فنّاوری اطلاعات، رشته تحصیلی، درجه سازمانی و رده شغلی بوده است.

در مواردی که اطلاعات از منابع ثانویه قابل استحصال بوده است، از روش کتابخانه‌ای استفاده شده است. همچنین به منظور بررسی فرضیه‌های تحقیق، پرسشنامه‌ای بر اساس ادبیات موضوع و نظر خبرگان در این زمینه، در قالب ۷۰ پرسش به صورت طبقه‌بندی شده در ۹ مؤلفه آگاهی از امنیت اطلاعات در سه سطح دانش، نگرش و رفتار و بر اساس مقیاس لیکرت، ۱ به عنوان کاملاً مخالف تا ۵ به عنوان کاملاً موافق طراحی شد. پرسشنامه‌ها به صورت دستی توزیع و جمع‌آوری شد.

جامعه آماری مورد مطالعه در این پژوهش کارمندان ادارات ستادی سازمان پست بانک (۴۰۰ نفر) منظور شده است. برای انتخاب نمونه از روش نمونه گیری تصادفی ساده استفاده شد. در نمونه‌گیری تصادفی ساده، هر یک از عناصر جامعه مورد نظر برای انتخاب شدن شانس مساوی دارند. بر همین اساس ۲۰۰ نفر از کارمندان سازمان پست بانک انتخاب شدند.

با در نظر گرفتن امکان افت پرسشنامه ها، ۲۳۰ پرسشنامه توزیع و ۲۰۰ پرسشنامه قابل بررسی عودت داده شد. به هنگام توزیع پرسشنامه‌ها، توضیحاتی در رابطه موضوع پرسشنامه و اهمیت آن در سازمان، به صورت شفاهی و کتبی داده شد.

برای آزمون نرمال بودن متغیرها، از آزمون کولموگروف- اسمیرنوف استفاده شده است.

جدول ۱. نتایج آزمون نرمال بودن متغیرها

متغیر	سطح معنی‌داری	مقدار خطا	تأیید فرضیه	نتیجه گیری
(آگاهی از مؤلفه‌های امنیت اطلاعات)	۰/۴۴۶	۰/۰۵	H_0	نرمال است
(آگاهی از مؤلفه‌های امنیت اطلاعات در سطح دانش)	۰/۰۵۸	۰/۰۵	H_0	نرمال است
(آگاهی از مؤلفه‌های امنیت اطلاعات در سطح نگرش)	۰/۵۳	۰/۰۵	H_0	نرمال است
(آگاهی از مؤلفه‌های امنیت اطلاعات در سطح رفتار)	۰/۷۲۱	۰/۰۵	H_0	نرمال است

از آنجایی که مقدار سطح معنی‌داری کلیه متغیرها بزرگ‌تر از مقدار خطا۰/۰۵ است پس فرض صفر را نتیجه می‌گیریم یعنی توزیع همه متغیرها نرمال بوده است.

روایی پرسشنامه توسط تعدادی از اساتید و کارشناسان خبره در امر امنیت اطلاعات تأیید شد و از ضریب آلفای کرونباخ (یکی از متداول‌ترین روش‌های اندازه‌گیری[1] پایایی پرسشنامه) جهت تعیین پایایی پرسشنامه استفاده شد. پیش از توزیع کلی پرسشنامه‌ها، ابتدا ۲۰ پرسشنامه به صورت تصادفی بین اعضای نمونه توزیع شد تا پایایی پرسشنامه محاسبه شود.

جدول ۲. آزمون آلفای کرونباخ برای پایایی پرسشنامه

تعداد نمونه اولیه	تعداد سؤالات	مقدار آلفای کرونباخ
۲۰	۷۰	۰/۸۴۵۲

مقدار آلفای کرونباخ پرسشنامه بزرگ‌تر از مقدار ۰/۷ است و نشان می‌دهد پرسشنامه از پایایی خوبی برخوردار بوده است.

1. Measurement

روش‌های آماری بکارگرفته در این تحقیق شامل آمار توصیفی برای سؤالات جمعیت شناختی و تعیین میانگین امتیاز برای کلیه شاخص‌ها و جهت آزمون فرضیه‌های تحقیق، از آزمون‌های ضریب همبستگی کرامر، ضریب همبستگی اسپیرمن، ضریب همبستگی پیرسون استفاده شده است.

یافته‌های پژوهش

بر اساس آمار توصیفی، امتیاز و اولویت هر یک از مؤلفه‌ها در جدول زیر(بر حسب درصد) آورده شده است.

جدول ۳ . نتایج ارزیابی پرمایگی آگاهی از امنیت اطلاعات کارمندان

راهنمای جدول ۳	
نارضایت‌بخش	۵۹-۰
نیاز به آموزش و بررسی	۷۹-۶۰
رضایت‌بخش	۱۰۰-۸۰

	دانش	نگرش	رفتار	آگاهی از هر مؤلفه	اولویت مؤلفه‌ها برای آموزش
مؤلفه ۱: ایمیل و ضمایم و اسپم	۰۲۵/۶۸	۵۳	۶۸	۱۳۲/۶۳	۵
مؤلفه ۲: پشتیبانی	۱۸۵/۷۹	۵۶/۶۸	۱۶۷/۶۹	۳۵۴/۷۲	۹
مؤلفه ۳: رمز عبور	۴۵۷/۷۳	۳۷۵/۸۳	۵/۵۷	۴۴۵/۷۱	۸
مؤلفه ۴: مهندسی اجتماعی	۷۵/۶۶	۵۹	۷۵/۵۹	۷۵/۶۱	۲
مؤلفه ۵: امنیت در انتقال اطلاعات	۹۳۷/۵۸	۳۵۷/۶۲	۹۵۷/۸۲	۰۹/۶۸	۷
مؤلفه ۶: بدافزارها	۲۷/۶۹	۳۷۵/۶۹	۰۶۲/۶۷	۹۰/۶۷	۶
مؤلفه ۷: اینترنت	۹۸/۴۸	۶۲۵/۷۰	۲۲/۶۷	۲۷۵/۶۲	۴
مؤلفه ۸ :گزارش دهی	۸۳۲/۵۵	۰/۶۵	۰۸۳/۵۳	۹۷۲/۵۷	۱
مؤلفه ۹ : التزام به سیاست‌های سازمان	۲۵/۶۱	۵۰/۶۳	۰/۶۴	۰۱۷/۶۲	۳
	آگاهی در سطح دانش ۵۹/۶۴	آگاهی در سطح نگرش ۸۶۷/۶۵	آگاهی در سطح رفتار ۴۷/۶۵	آگاهی کلی از مؤلفه‌ها ۳۱/۶۵	

با توجه به جدول ۳، میزان آگاهی کلی کارمندان در سطوح دانش، نگرش و رفتار در سطح متوسط است و کارمندان در سطح دانش نسبت به دو سطح نگرش و رفتار در وضعیت پایین‌تری قرار دارند و سطح نگرش آنها نسبت به مؤلفه‌های امنیت اطلاعات در وضعیت نسبتاً بهتری نسبت به رفتار است. در جدول فوق، میزان آگاهی کارمندان در کلیه مؤلفه‌ها در سه سطح آمده است به طوری در نواحی که امتیاز آنها از ۶۰ کمتر باشد، میزان آگاهی کارمندان در وضعیت نامطلوب قرار دارد و در نواحی امتیاز آنها بین ۶۰ تا ۸۰ باشد، نیاز به توجه و برنامه‌ریزی بیشتری دارند و در نواحی بالاتر از ۸۰ وضعیت مطلوب تلقی می‌شود. آگاهی کلی کارمندان از کلیه مؤلفه‌های امنیت اطلاعات، دارای امتیاز ۶۵/۳۱ است که نشان می‌دهد مدیران سازمان و مسؤولین امنیت اطلاعات بایستی، تلاش و برنامه‌ای مدون و مناسب بر اساس نتایج تحقیق، جهت ارتقاء سطح آگاهی کارمندان از امنیت اطلاعات در پیش بگیرند.

ستون آخر نیز اولویت مؤلفه‌هایی را که نیاز به آموزش و توجه بیشتر است نشان می‌دهد. در این مؤلفه‌ها، نیاز به آموزش و توجه در مؤلفه گزارش‌دهی از همه بیشتر و به همین ترتیب در مؤلفه‌های رمز عبور و پشتیبانی نسبت به بقیه کمتر است. اولویت نیاز به آموزش و توجه بیشتر مؤلفه‌ها به ترتیب عبارتند از:

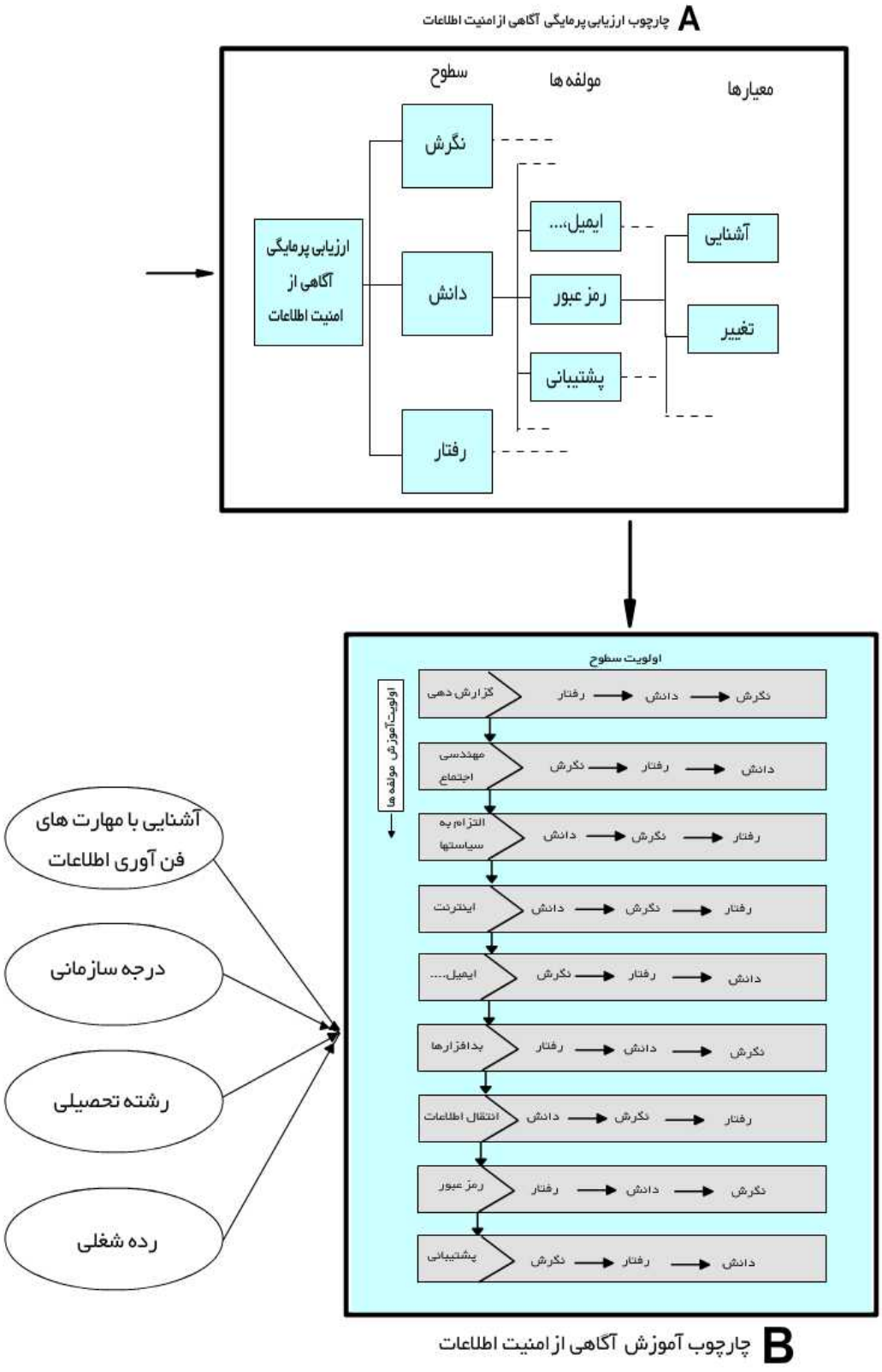
۱. گزارش‌دهی
۲. مهندسی اجتماعی
۳. التزام به سیاست‌های امنیتی سازمان
۴. اینترنت
۵. ایمیل، ضمایم و هرزنامه
۶. بدافزارها
۷. انتقال ایمن اطلاعات
۸. رمز عبور
۹. پشتیبانی

نمودار ۱ . میزان آگاهی کارمندان از مؤلفه‌های امنیت اطلاعات

برای آزمون فرضیه‌ها، از آزمون‌های ضرایب همبستگی کرامر و اسپیرمن استفاده شد که نتایج آن در جدول زیر نشان شده است.

جدول ٤ . ضرایب همبستگی بین متغیرهای مستقل و متغیر وابسته (آگاهی از مؤلفه‌های امنیت اطلاعات)

متغیر مستقل	سطح معنی‌داری	مقدار خطا	نتیجه‌گیری	مقدار ضریب همبستگی
۱- جنسیت	۰/۶۶۹	۰/۰۵	عدم وجود همبستگی	۰/۰۸۵
۲- میزان تحصیلات کارکنان	۰/۳۰۸	۰/۰۵	عدم وجود همبستگی	۰/۰۷۲
۳- آشنایی با مهارت‌های فنّاوری اطلاعات	۰/۰۰۲	۰/۰۵	وجود همبستگی	۰/۲۱۶
۴- سابقه کاری کارکنان	۰/۱۰۹	۰/۰۵	عدم وجود همبستگی	-۰/۰۹
۵- درجه سازمانی	۰/۰۱۰	۰/۰۵	وجود همبستگی	۰/۱۸۲
۶- رشته تحصیلی	۰/۰۰۲	۰/۰۵	وجود همبستگی	۰/۳۲۴
۷- رده شغلی	۰/۰۰۶	۰/۰۵	وجود همبستگی	۰/۲۱۲



شکل ٤. چارچوب مفهومی ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کارمندان

با استفاده از جدول ۴، مشخص می شود که فرضیه‌های ۱،۲ و ۴ تأیید نشده و فرضیه‌های ۳، ۵، ۶ و ۷ تأیید شدند. با استفاده از این نتایج، مسؤولین ذیربط قادر هستند برنامه‌های آموزشی لازم در جهت ارتقای میزان آگاهی از امنیت اطلاعات کارمندان را در سطوح لازم و اولویت مؤلفه‌های تعیین شده امنیت اطلاعات، مطابق با جدول و با در نظر گرفتن عوامل مؤثر در آن، به نحوی مطلوب‌تر و مفیدتر تدوین کرده، ارائه دهند. برای این منظور و ارائه بسترهای علمی مناسب، چارچوب زیر به عنوان چارچوب مفهومی ارزیابی و آموزش پرمایگی امنیت اطلاعات کارمندان ارائه می‌شود.

نتیجه گیری

سازمان‌ها بایستی علاوه بر سرمایه‌گذاری بر راه‌حل‌های فنی برای حفظ امنیت اطلاعات، به عوامل غیر فنی و انسانی از جمله ارتقاء سطح آگاهی کلیه کارمندان از مؤلفه‌های امنیت اطلاعات، توجه بیشتری داشته باشند. برای این منظور لازم است مسؤولین ذیربط در حیطه فنّاوری اطلاعات، یک چارچوب مناسب در جهت ارزیابی میزان آگاهی کارمندان و آموزش امنیت اطلاعات پیش‌رو داشته باشند و با استفاده از این چارچوب و با در نظر گرفتن اولویت مؤلفه‌ها، اولویت سطوح (دانش، نگرش و رفتار) هر مؤلفه و عوامل مؤثر در آن قادر خواهند بود برنامه‌های آموزشی آگاهی از امنیت اطلاعات را به نحوی مؤثرتر و مفیدتر ارائه دهند.

منابع

شیرازی، حسن، آل‌شیخ، روح الله (۱۳۸۹). *مدیریت امنیت اطلاعات (جلد دوم)*. تهران: دانشگاه مالک اشتر.

طاهری، مهدی(۱۳۸۶). *ارائه چارچوبی برای نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی* (پایان‌نامه کارشناسی ارشد). دانشگاه تربیت مدرس، تهران

Choi, Namjoo, Kim, Dan, and Goo, Jahyun (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security, 16*, 484-485.

Chang, Ernest, Lin, Chin-Shien (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*, 1-10.

Crowston, K. & Williams, M.(2000). Reproduced and emergent genres of communication on the World-Wide Web. *The Information Society, 16*(3), 201–215,

Kritzinge, E. and Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computer & security,27*, 224-231.

Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computer & security, 25*, 289-296.

Kruger, H.A., Drevin, L. and Steyn, T. (2010). A Vocabulary test to assess information. Information Management & Computer Security Journal,. 18(5), 316-19.

Maconachy, W. V., Schou, C. D., Ragsdale, D., Welch, D. (2001). *A Model for Information Assurance - An Integrated Approach*. Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, June, 5-6.

Nikrerk J.F. and Solms, Van (2009). Information security culture: a management perspective. *Computer & security, 5*, 142-144.

Shaw, Samuel C., Charlie, C. and Chen, R.S. (2002). Mitigating Information Security Risks by Increasing User Security Awareness - Case Study of an Information Security Awareness System. *Information Technology, Learning, and Performance Journal, 24*,132-133.

Shaw, R.S., Charlie, C., Harris, Albert. and Huang, Hui-Jou (2009). The impact of information richness on information security awareness training effectiveness. *Computer & Education, 52*, 93-100.

Von Solms R, Von Solms B. (2004). Information security management (1): Why information security is so important. Information Management and Computer Security, Vol. 6, PP. 174 –77.

Stanton, J. M., Stam, K.R., Mastrangelo, P. and Jolton, j. (2005). Analysis of end user security behaviours. *Computer & Security, 24*,124-33.

Thomson, M.E. and Von Solms, R. (1998). Information security awareness - educating your users effectively. *Information Management & Computer Security, 6*(4), 167-173.

Veiga, A. Da., and Eloff, J.H.P. (2010). A Framework and Assessment Instrument for Information Security Culture. *Compuer & Security, 29*(2), 196-200.

Von Solms, B. (2000). Information security - the third wave. *Computers & Security,19*, PP. 15–19.

Wilson, Mark, and Hash, Joan. (2003). Building an information technology security awareness and training program. *National Institute of Standards and Technology*, sp 800-50, 20-79.

Wood, C.C (1994). *Information security policies made easy*. Ohio: Bookmaster.