
بسم الله الرحمن الرحيم

مرکز تهران

پایان‌نامه برای دریافت درجه کارشناسی ارشد

در رشته مدیریت فن‌آوری اطلاعات

دانشکده فنی و مهندسی

گروه علمی مهندسی کامپیوتر و مدیریت فن‌آوری اطلاعات

عنوان پایان‌نامه:

ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران (مورد مطالعه: پست بانک)

نگارش:

نرگس جهانگیری

استاد راهنما:

دکتر محمد حسن زاده

استاد مشاور:

دکتر داوود کریم زادگان مقدم

این پایان‌نامه مورد حمایت مالی سازمان پست‌بانک قرار گرفته است.

مهرماه ۱۳۹۰

تقدیم به:

پدر و مادر، همسر عزیز و فرزندانم

تشکر و قدردانی

دل هر ذره را که بشکافی آفتابیش در میان بینی

اول از خداوند بزرگ سپاس‌گزارم که همواره بهترین‌ها را برایم خواسته است. بر خود واجب می‌دانم که از زحمات بی‌دریغ، تلاش بی‌وقفه و راهنمایی‌های راه‌گشای استاد ارجمند جناب آقای دکتر حسن زاده در طول این پروژه تشکر و قدردانی به عمل آورم. همچنین از زحمات استاد محترم جناب آقای دکتر کریم‌زادگان که با راهنمایی‌های خود راه‌گشای اینجانب بوده‌اند، تشکر می‌نمایم. از پدر و مادر عزیز و گرامی‌ام که همواره در طول تحصیل مشوق و پشتیبان من بوده‌اند تشکر نموده و سلامتی آن‌ها را از خداوند متعال خواستارم. از همسر عزیزم، به خاطر تمام سختی‌هایی که در طول این تحقیق ناگزیر بر ایشان گذشت و بدون هرگونه شکوه‌ای همواره یاور و حامی من بوده‌اند، قدردانی می‌نمایم. امیدوارم بتوانم قدردان زحمات ایشان باشم.

در پایان از کلیه عزیزانی که به هر شیوه ممکن در انجام این پروژه کمک و یاری رسانده‌اند، تشکر می‌نمایم.

نرگس جهانگیری

چکیده

با توجه ویژگی‌های عصر امروزی که عصر اطلاعات نیز نامیده شده است، مهم‌ترین سرمایه برای هر فرد و یا سازمان، اطلاعات است به همین جهت، امنیت اطلاعات جزء یکی از مهم‌ترین مسائل امروزی گشته است. بیشتر حوادث نقض امنیت اطلاعات، به دلیل عدم توجه به نیروی انسانی علیرغم راه‌حل‌های فنی است. تحقیقات گذشته نشان می‌دهد یکی از فاکتورهای موثر در عوامل انسانی موضوع آگاهی و اطلاع‌رسانی به کاربران از امنیت اطلاعات است. آموزش و آگاهی‌رسانی بایستی یکی از پایه‌ها و سرفصل‌های برنامه‌های امنیتی هر سازمان قرار گیرد. فقدان این مسئله در سازمان‌های دولتی به شدت مشهود است، همین‌طور در سطح اجتماع در حالی که نفوذ کامپیوتر به سرعت ادامه دارد، روند برنامه‌های آموزش و اطلاع‌رسانی به کندی پیش می‌رود. این امر باعث شده که کارکنان سازمان‌ها از حداقل آگاهی‌ها و تدابیر دفاعی لازم آگاه نباشند.

با توجه به اینکه در بیشتر تحقیقات گذشته، آگاهی از امنیت اطلاعات کاربران مورد توجه قرار نگرفته است. در این تحقیق، میزان سطح آگاهی از امنیت اطلاعات کاربران در سه سطح دانش، نگرش و رفتار مورد ارزیابی قرار گرفت و برای محاسبه سطح آگاهی از امنیت اطلاعات کارمندان، ۹ مؤلفه بررسی شد. عوامل متنوعی بر که بر میزان آگاهی کاربران از امنیت اطلاعات به عنوان متغیر وابسته این تحقیق، تأثیر گذار است، شناسایی شد که شامل ۷ متغیر مستقل جنسیت، میزان تحصیلات، میزان آشنایی با مهارت فن‌آوری اطلاعات، میزان سابقه شغلی، درجه سازمانی، رشته تحصیلی و رده شغلی کارمندان است. پرسشنامه نیز با کمک خبرگانی در زمینه امنیت اطلاعات تجدید نظر شده و مقیاس لیکرت ۵ امتیازی از ۱، به عنوان کاملاً مخالف تا ۵، به عنوان کاملاً موافق برای اندازه‌گیری منظور گردید و با استفاده از آزمون ضریب همبستگی اسپیرمن و کرامر و پیرسون ارتباط بین متغیرهای مستقل و متغیر وابسته در سطح معناداری ۰,۰۵ سنجیده شد. جامعه آماری، کارکنان ادارات ستادی پست بانک بودند و نمونه ۲۰۰ نفر انتخاب گردید. ضمن آنکه آلفای کرونباخ پرسشنامه نمونه اولیه به دست آمده، نشان از پایای مناسب آن بود. نتایج آشکار کرد که از ۷ متغیر مستقل فقط متغیرهای درجه سازمانی، آشنایی با مهارت‌های فن‌آوری اطلاعات، رشته تحصیلی و رده شغلی در سطح معناداری با متغیر وابسته آگاهی از امنیت اطلاعات دارای همبستگی است.

کلمات کلیدی

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

فهرست مطالب

فهرست جداول

فهرست شکل‌ها

فصل اول

کلیات تحقیق

۱ ـ ۱ مقدمه

در سال‌های اخیر با پیشرفت تکنولوژی اطلاعات[1] و ارتباطات[2] شاهد به‌کارگیری تجهیزات الکترونیک 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[3]، اختلال در ارائه خدمات اطلاع‌رسانی یا نظارتی و نقض حقوق مالکیت معنوی است.

از طرف دیگر با رشد و توسعه فزاینده فن‌آوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری[4] فضای تبادل اطلاعات افزایش یافته است و روش‌های اعمال تهدیدهای یاد شده، گسترده‌تر و پیچیده‌تر می‌شود. از این رو حفظ ایمنی فضای تبادل اطلاعات از جمله مهم‌ترین اهداف توسعه فن‌آوری اطلاعاتی و ارتباطی محسوب می‌شود (Wilson and Hash, 2003; Kruger and Kearmey, 2006; Veiga and Eloff, 2010).

بررسی‌های موسسه‌های expo storage حاکی از آن است که ۸۳ درصد شرکت های تجاری برای حفظ امنیت اطلاعات ذخیره شده خود برنامه خاصی ندارند و در صورت از بین رفتن این اطلاعات در اثر خراب‌کاری یا نفوذ هکرها و کلاه برداران به سیستم های رایانه‌ای به سختی می‌توانند این اطلاعات را بازیافت کنند. همچنین در گزارشی دیگر عدم توجه و سهل‌انگاری کاربران را خطرناک‌تر از حملات هکرها اعلام کردند (Santa, 2008).

به طور کلی امنیت اطلاعات، به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیر مجاز اشاره دارد (Von Solms, 2000)، همچنین مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری (خالقی، ۱۳۸۳) و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیر مجاز است (Wilson and Hash, 2003). با توجه به تعاریف ارائه شده، امنیت به مجموعه‌ای از تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیر مجاز در نظام‌های رایانه‌ای و ارتباطی اطلاق می‌شود.

یکی از جنبه‌ها و راه‌های غیر فنی[5] برای حفاظت و مدیریت امنیت اطلاعات ارتقاء آگاهی[6] کاربران از امنیت اطلاعات است در این صورت افراد، آگاه به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود هستند. آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و

1 Information Technology
2 Comminucation
3 Data Base
4 Vulnerability
5 Non Technical
6 Awareness

تقویت فعالیت‌های خوب امنیتی[1] می‌شود و به افراد اجازه می‌دهد تا نسبت به امنیت فن‌آوری اطلاعات نگران و پاسخگو باشند (Wilson and Hash, 2003) و به تدریج به فرهنگ[2] در سازمان‌ها تبدیل خواهد شد (Kruger and Kearrney, 2006; Nikerk and Solms, 2009).

لذا بایستی به موازات تمهیدات فنی[3] اعمال شده جهت امنیت اطلاعات، در قوانین و سیاست‌های جاری متناسب با جایگاه نوین فضای تبادل اطلاعات در امور مدیریتی و اطلاع‌رسانی تجدید نظر شده و فرهنگ و آموزش‌های صحیح به‌کارگیری اطلاعات و تأمین امنیت آن‌ها در اولویتی بالاتر نیز در سطح جامعه ترویج شود.

۱ ۲ بیان مسئله

با افزایش وسعت شبکه‌ها و دسترسی آسان به اینترنت، خطرات امنیتی نیز به سرعت بیشتر و بیشتر می‌شوند. طی تحقیقی پیرامون موضوع آگاهی از امنیت اطلاعاتی کاربران معلوم شد که در سال‌های بین ۲۰۰۴ تا ۲۰۰۶ میزان متوسط زیان و تعداد قانون شکنی‌های امنیتی به حد چشمگیری کاهش پیدا کردند (Shaw et al., 2009). یکی از دلایل اصلی این ارتقاء در مشکل امنیتی، سرمایه‌گذاری‌های مستمر شرکت‌های کوچک و متوسط در فن‌آوری امنیت اطلاعات و برنامه‌های آگاهی از امنیت اطلاعات است (Shaw et al., 2009). کارمندان فن‌آوری اطلاعات به تنهایی در متوقف سازی رخداد قانون شکنی‌های امنیتی نمی‌توانند موثر باشند (Shaw and Charlie, 2002) لذا آگاهی امنیتی کاربران نهایی باید ارتقاء داده شود و یک توازن بین راه‌حل‌های فنی و غیر فنی در سازمان وجود داشته باشد (Kruger and Kearney, 2006).

بدیهی است که توجه نکردن به مقوله امنیت اطلاعات و افزایش ندادن آگاهی‌های لازم برای امنیت اطلاعات متناسب با سطوح مختلف افراد مانع از گسترش فضای اطلاعاتی در میان آحاد جامعه و جلب اعتماد مدیران در به‌کارگیری روش‌های نوین نظارتی و اطلاع‌رسانی خواهد شد. ایجاد یک چارچوب کلی در سطح کلان با لحاظ کردن ویژگی‌های خاص فضای تبادل اطلاعات و مقوله امنیت در این فضا یک ضرورت است.

هرچند در بیشتر سازمان‌ها در سطوح مختلف کاری اعم از وزارتخانه‌ها، سازمان‌های دولتی، نهادهای آموزشی و دیگر ارگان‌ها تدابیر و فرایندها، سیاست‌ها و استانداردهای مختلفی را پذیرفته و اجرا کرده‌اند ولی همچنان شاهد نقض امنیت اطلاعاتی در اکثر سازمان‌ها و نهادها می‌باشیم؛ و به نظر می‌رسد توجه لازم به تمام ابعاد مدیریت امنیت از جمله بخش عوامل انسانی نشده است

در این تحقیق پژوهشگر مؤلفه‌های موثر در ارزیابی[4] پرمایگی[5] و آموزش آگاهی از امنیت کاربران را شناسایی کرده و پس از بررسی اعتبار، یک چارچوب کلی برای ارزیابی پرمایگی آگاهی از امنیت

1 Good security activities
2 Culture
3 Technical
4 Assess
5 Richness

اطلاعات را ارائه می‌دهد. در این چارچوب سه سطح از آگاهی امنیتی که عبارتند از: دانش[1]، نگرش[2] و رفتار[3]، مورد توجه قرار می‌گیرد (Kruger and Kearney, 2006).

با افزایش دانش و آگاهی‌های کارمندان یک سازمان از امنیت اطلاعات در راستای این سه سطح، میزان پرمایگی دانش امنیت اطلاعات از جانب افراد بالاتر می‌رود. رعایت اصول امنیتی در افراد به تدریج به صورت نهادینه و رفتاری تبدیل می‌شود؛ و این امر به تغییر فرهنگ‌ها و ارزش‌های امنیتی کمک کرده و از این طریق صلاحیت امنیتی بهتری ایجاد می‌شود. اگرچه روشی واحد که با تمامی موقعیت‌ها منطبق باشد در سطح سازمانی و انسانی در عملکردهای مختلف برنامه‌های مربوط به ارزیابی و ارتقاء آگاهی امنیتی یکسانی جود ندارد، داشتن یک رویه مشخص برای برقراری برنامه‌های ارزیابی و ارتقاء بر اساس سطوح آگاهی امنیتی بسیار ضروری است .

۱ ۳ سوالات تحقیق

۱. مؤلفه‌های آگاهی از امنیت اطلاعات کارکنان کدام است؟
۲. چه عواملی بر سطح آگاهی از مؤلفه‌های امنیت اطلاعات کارمندان در یک سازمان عینی تأثیرگذار است؟
۳. آیا بین سطوح آگاهی از امنیت اطلاعات (دانش، نگرش و رفتار) ارتباط وجود دارد؟

۱ ۴ فرضیه‌ها

هفت فرضیه اول مربوط به سوال دوم است و فرضیه ۸ مربوط به سوال سوم می‌باشد.

- فرضیه (۱) : بین جنسیت کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
- فرضیه (۲) : بین میزان تحصیلات کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
- فرضیه (۳) : بین مهارت‌های فن‌آوری اطلاعات کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
- فرضیه (۴) : بین سابقه خدمت کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
- فرضیه (۵) : بین درجه سازمانی کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.

1 knowledge
2 Attitude
3 Behavior

- فرضیه (۶) : بین رشته تحصیلی کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
- فرضیه (۷) : بین رده شغلی کارکنان و پرمایگی آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها، همبستگی وجود دارد.
- فرضیه (۸) : بین سطوح آگاهی از امنیت اطلاعات (دانش، نگرش و رفتار) همبستگی وجود دارد.

۱ ۵ اهداف پژوهش

۱ ۵ ۱ اهداف آرمانی

- رسیدن به یک جامعه اطلاعاتی ایمن و مطمئن.
- تقویت بنیه‌ی دولت الکترونیکی و کاهش جرایم اینترنتی.
- مقابله با سوءاستفاده‌های ناشی از ناآگاهی کاربران از مسائل امنیت اطلاعات.

۱ ۵ ۲ اهداف اصلی

- ارائه یک چارچوب برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران در سازمان‌ها.
- کمک به رسیدن به سطح قابل قبولی از امنیت به موازات پذیرش راه‌حل‌های فنی در حفظ اطلاعات به عنوان باارزش‌ترین سرمایه سازمان.

۱ ۵ ۳ اهداف ویژه

- تعیین همبستگی جنسیت با میزان آگاهی از مؤلفه‌های امنیت اطلاعات کارمندان.
- تعیین همبستگی سطح با نوع تحصیلات کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.
- تعیین همبستگی مهارت فن‌آوری اطلاعات کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.
- تعیین همبستگی سابقه خدمت کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.
- تعیین همبستگی درجه سازمانی کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.
- تعیین همبستگی رده شغلی کارکنان با میزان آگاهی از مؤلفه‌های امنیت اطلاعات آن‌ها.

- تعیین اولویت‌بندی مؤلفه‌های امنیت اطلاعات در یک محیط سازمانی (عینی).
- شناخت ارتباط بین سطوح آگاهی از امنیت اطلاعات کارمندان.

۱ ۶ نوآوری تحقیق

بیشتر تحقیقات در زمینه امنیت اطلاعات بر روی عوامل فنی تاکید دارند و کمتر به عوامل غیر فنی پرداخته می شود. طبق تحقیقات انجام شده آگاهی و آموزش کاربران از امنیت اطلاعات یکی از فاکتورهای شناخته شده از عوامل غیر فنی تاثیرگذار بر امنیت اطلاعات سازمان است. تاکید این تحقیق بر ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کارمندان در سازمان‌ها، نوآوری آن محسوب می‌شود که در صورت ارائه می‌تواند به عنوان نقشه راهی برای همه سازمان‌ها جهت ارزیابی و ارتقاء دانش کارمندان از امنیت اطلاعات تلقی شود.

۱ ۷ ضرورت و سابقه تحقیق

امروزه امنیت از اطلاعات به عنوان مهم‌ترین چالش سازمان‌هایی که در تلاش هستند از فرصت‌های فن‌آوری اطلاعات بهره‌امند شوند، مطرح است و برای بهره‌مندی از فرصت‌های فاوا باید به امنیت اطلاعات فراتر از فن‌آوری و در قالب یک فرهنگ نگریست (طاهری، ۱۳۸۶). در واقع امنیت باید در یک سازمان تبدیل به یک فعالیت و فرآیند دائمی جهت مدیریت مخاطرات شود که پوشش دهنده مجموعه منابع اطلاعاتی، فن‌آوری‌ها، انسان‌ها و فرآیندهایی است که به این منابع مرتبط می‌باشند. یکی از راه‌های کم هزینه و موثر در رسیدن به این آرمان افزایش سطح آگاهی کاربران از امنیت اطلاعات و مخاطرات آن است. موضوعی که معمولاً به سادگی از کنار آن می‌گذرند در صورتی که باید در کنار راه‌حل‌های فنی و سیاست‌ها در جهت رسیدن به سطح قابل قبولی از امنیت، مورد توجه ویژه قرار گیرد (Kruger and Kearney, 2006).

بسیاری از سازمان‌ها به اهمیت برقراری یک برنامه برای ارزیابی و آگاهی رسانی پیرامون امنیت اطلاعاتی در سازمان‌هایشان پی برده‌اند. بالا رفتن آگاهی امنیتی افراد می‌تواند به تغییر فرهنگ‌ها و ارزش‌های امنیتی کمک کرده و از این طریق صلاحیت امنیتی بهتری ایجاد می‌شود و سازمان، بیشترین منفعت را از به‌کارگیری فن‌آوری اطلاعات و ارتباطات را در جهت رشد و ترقی خواهد داشت. اگرچه روشی واحد که با تمامی موقعیت‌ها منطبق با سطح سازمانی و انسانی در عملکردهای مختلف برنامه‌های مربوط به آگاهی امنیتی وجود ندارد. داشتن یک روش مشخص برای برقراری یک برنامه برای ارزیابی و ارتقاء دانش کاربران از امنیت اطلاعات امنیتی بر اساس این سطوح بسیار ضروری است.

مفهوم و اهمیت ایمنی و امنیت از همان آغاز زندگی بشر وجود داشت، بشر همیشه برای بقا و ادامه زندگی سعی نموده است که آگاهی‌ها و دانش خود را نسبت به محیط و خطرات اطراف خود افزایش دهد. ایمنی و امنیت یک مفهوم ذاتی است که با حفاظت از چیزهای ارزشمند ارتباط پیدا می‌کند؛ و به طور خلاصه ایمنی به راه‌های ممکن که در آن سلامت یک سیستم بایستی تأمین و دفع نقایصی که در راه حصول به اهداف وجود دارد تعریف می‌شود (سادوسکای، ۱۳۸۴).

امروزه در هر لحظه با سر زدن به هر یک از سایت‌های خبر گزاری شاهد نقض امنیت و جرایم اینترنتی، کلاه برداری از حساب‌های شخصی و دولتی و هک شدن تعداد بی‌شماری از سایت‌های حقیقی و حقوقی و غیره می‌باشیم، می‌توان با توجه به این اخبار و ارقام به این نتیجه رسید که امنیت اطلاعات هنوز جایگاه خود را نیافته است هر چند در انتهای دهه ۱۹۸۰ استانداردهای مختلفی برای امنیت اطلاعات همچون، ISO/IEC 27001 , ISO/IEC TR13335, BS7799ایجاد شد و خیلی از سازمان‌ها با پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات (ISMS) برای ارزیابی امنیت سیستم‌های اطلاعاتی تا حدودی امنیت اطلاعات را برای خود تأمین کردند (پاکدامن، ۱۳۸۸). از سال ۲۰۰۰ تا به این زمان، تحقیقات متعددی در ارتباط با ارزیابی و آگاهی از امنیت اطلاعات انجام شده است که در ادامه ارائه شده است.

ماکوناچی[1] و همکارانش در سال ۲۰۰۱ ابعاد مهم در امنیت اطلاعات را مورد توجه قرار داده‌اند. توجه به مشخصات اصلی امنیت اطلاعات (در دسترس بودن، صحت، قابلیت اعتماد) و اقدامات امنیتی (تکنولوژی، 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[2] در تحقیق، به عمل آمده در سال ۲۰۰۶ در زمینه ارزیابی میزان آگاهی از امنیت اطلاعات در شرکت‌های بین‌المللی معادن، نتایج به دست آوردند. آن‌ها سطوح آگاهی از امنیت اطلاعات را در سه سطح دانش، نگرش و رفتار تقسیم کردند و به این نتیجه رسیدند که در کل، سطح آگاهی کارمندان در حد متوسطی قرار دارد که نیاز به آموزش و توجه بیشتری دارد. پژوهش دیگری که در سال ۲۰۰۷ توسط چانگ[3] انجام شد نیز ثابت شد فرهنگ سازمانی، تأثیر مستقیم بر ایجاد فرهنگ امنیت اطلاعات دارد. یکی از تحقیقات مهم در این زمینه در سال 2008 توسط چو[4] و همکارانش انجام شد، این 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 و عملکرد سازمان بهبود خواهد یافت.

در تحقیق دیگری با عنوان مدلی برای آگاهی و بازیابی امنیت اطلاعات توسط اسمیت و کریتزینگر[5] در سال 2008 انجام شد، بدنه کلی برای مدیریت امنیت مستخرج شده 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 توسط شو[6] و همکارانش در سال ۲۰۰۹ با عنوان بررسی ارزیابی غنای اطلاعاتی بر آگاهی از امنیت اطلاعات کاربران در محیط آن‌لاین است. وی آگاهی از امنیت اطلاعات را به سه سطح دریافت[7]، درک[8] و برون

1 Maconachy
2 Kruger & Kearney
3 Chang Ernest
4 Choi Namjoo
5 E. kritzinger and E Smith
6 Shaw
7 Perception
8 Comprehension