

اولویت بندی عوامل موثر بر امنیت اطلاعات الکترونیکی سلامت در مراکز درمانی*

مهدی کاهویی^۱، زینب عباسی^۲

مقاله پژوهشی

چکیده

مقدمه: استفاده از فناوری های جدید نگرانی های زیادی در مورد حفظ حریم شخصی و تامین امنیت اطلاعات سلامت به وجود آورده است. با توجه به اینکه کارکنان مراکز درمانی، کاربران اصلی سیستم اطلاعات بیمارستان هستند که هدف آن بهبود کیفیت ارائه مراقبت می باشد، از این رو هدف از این مطالعه شناسایی دیدگاه کارکنان نسبت به امنیت اطلاعات الکترونیکی سلامت بود.

روش بررسی: این مطالعه توصیفی روی ۴۰۰ نفر از کارکنان شاغل در مراکز درمانی دانشگاه علوم پزشکی سمنان در سال ۹۱-۹۲ خورشیدی انجام شد. داده ها بوسیله یک پرسشنامه پژوهشگر ساخته که روایی آن براساس تایید صاحب نظران و پایایی آن بر اساس آزمون و بازآزمون تایید شده بود، جمع آوری و بوسیله آزمون های آمارهای توصیفی تجزیه و تحلیل شدند.

یافته ها: یافته ها نشان داد ۵/۷ درصد کارکنان نقش کاربران سیستم های اطلاعاتی، ۳۸/۳ درصد درک اهمیت امنیت اطلاعات، ۳۳ درصد آموزش ضمن خدمت و ۴۷/۵ درصد وجود زیر ساخت مناسب را از مهمترین عوامل امنیت اطلاعات سلامت انتخاب کردند.

نتیجه گیری: نتایج نشان داد کارکنان رعایت عوامل سازمانی، رفتاری و غیره را مهمترین اولویت های امنیت اطلاعات سلامت در نظر داشتند. به نظر می رسد جهت افزایش ضریب امنیت اطلاعات الکترونیکی سلامت در مراکز درمانی ایجاد سیاست های کنترلی، برگزاری دوره های آگاه سازی، سرمایه گذاری در موارد فنی و ایجاد زیرساخت مناسب برای بهبود امنیت اطلاعات سلامت ضروری باشد.

واژه های کلیدی: سیستم های اطلاعات سلامت؛ امنیت داده ها؛ مراکز پزشکی دانشگاهی.

پذیرش مقاله: ۹۳/۴/۸

اصلاح نهایی: ۹۳/۴/۳

دریافت مقاله: ۹۲/۱۲/۱۴

ارجاع: کاهویی مهدی، عباسی زینب. اولویت بندی عوامل موثر بر امنیت اطلاعات الکترونیکی سلامت در مراکز درمانی. مدیریت اطلاعات سلامت ۱۳۹۴؛ ۱۲(۲): ۱۶۲-۱۷۰.

*- این مقاله حاصل پروژه کارشناسی رشته فناوری اطلاعات سلامت است.

۱- استادیار، مدیریت اطلاعات سلامت، مرکز تحقیقات عوامل اجتماعی موثر بر سلامت، گروه پیراپزشکی، دانشکده پرستاری و پیراپزشکی، دانشگاه علوم پزشکی سمنان، سمنان، ایران

۲- کارشناس، فناوری اطلاعات سلامت، کمیته تحقیقات دانشجویی، دانشگاه علوم پزشکی سمنان، سمنان، ایران (نویسنده مسؤول)

Email: Z.abasi6516@yahoo.com

مقدمه

در عصر حاضر سازمان‌های مراقبت سلامت با ارزش‌ترین دارایی خود را جهت پردازش و ذخیره سازی در اختیار فناوری اطلاعات قرار داده‌اند. وابستگی به این فناوری باعث شده است که اگر در ارایه خدمات سیستم‌های اطلاعاتی خللی پیش آید سازمان نتوانند به کار خود ادامه دهند. بدین ترتیب حیات سازمان‌های مراقبت سلامت ارتباط نزدیکی با سیستم‌های اطلاعاتی آنها دارد (۱،۲). سیستم‌های اطلاعاتی نیز همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در ارایه خدمات می‌باشند. از این رو سازمان‌ها برای ایمن ماندن از این آسیب‌ها باید به فکر امنیت اطلاعات باشند (۳،۴). امنیت اطلاعات به معنای کنترل دسترسی و حفظ اطلاعات از افشای تصادفی یا غیر عمدی به افراد غیر مجاز، جایگزینی، دستکاری یا فقدان اطلاعات می‌باشد (۵).

استفاده از این تکنولوژی‌های جدید نگرانی‌های زیادی در مورد حفظ حریم شخصی و تامین امنیت اطلاعات سلامت به وجود آورده است زیرا اطلاعات پزشکی بیمار شامل برخی از خصوصی ترین و محرمانه‌ترین اطلاعات بیمار بوده و اطلاعات رایانه‌ای از مکان‌های متعددی قابل دسترس است (۶). نقص امنیتی این سیستم‌ها خطر افشای اطلاعات را به دنبال خواهد داشت. به طوری که بررسی‌های انجام شده در آمریکا حاکی از آن است که ۷۵ درصد افراد از افشای غیرمجاز و به اشتراک گذاشتن اطلاعات بر روی شبکه‌ها و وب سایت‌ها نگرانند (۷،۳). یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقا آگاهی کاربران از امنیت اطلاعات است. برنامه آگاه سازی امنیتی کلیدی‌ترین عنصر در اجرای موفق یک سیاست امنیتی در کل سازمان است. هدف اصلی این برنامه تعریف نقش تک تک کارکنان در محافظت از منابع اطلاعاتی حیاتی سازمان است (۸،۹). در مطالعه‌ای که توسط Smit با عنوان آگاهی و بازیابی امنیت اطلاعات انجام شد نمای کلی برای مدیریت امنیت اطلاعات به دو قسمت فنی و غیر فنی تقسیم شد که از جمله

موضوعات غیر فنی تاثیرگذار برای امنیت اطلاعات، موضوع عوامل انسانی بود (۱۰). بسیاری از پژوهش‌ها نشان می‌دهند بیش از ۸۰ درصد مشکلات امنیتی در سازمان‌ها ناشی از خطاهای سهوی و عمدی کارکنان بوده است اما خطاهای سهوی اکثرا به دلیل عدم آگاهی به وجود می‌آید (۱۱،۹).

یکی از ابعاد مهم امنیت اطلاعات سلامت، حفظ تعادل بین امنیت سیستم اطلاعات مراقبت سلامت و قابلیت دسترسی داده‌ها به اطلاعات مراقبت سلامت است از سویی دیگر یکی از اهداف اصلی نگهداری اطلاعات سلامت و پرونده‌های پزشکی تسهیل مراقبت با کیفیت بالا برای بیماران است به عبارت دیگر اگر شیوه‌های امنیتی سازمان به قدری قوی باشد که مانع از دسترسی مناسب به اطلاعات مورد نیاز جهت مراقبت بیمار شود، این هدف مهم نادیده گرفته می‌شود و اگر هم سازمان اجازه دسترسی نامحدودی به همه‌ی کارکنانش بدهد، حقوق بیمار راجع به حریم خصوصی و محرمانگی نقض شده و سرمایه‌های فناوری اطلاعات سازمان در معرض خطر قابل توجهی قرار می‌گیرد (۱۲).

با توجه به اینکه مطالعات کمی در زمینه اولویت‌بندی دیدگاه کارکنان نسبت به امنیت اطلاعات سلامت در سیستم‌های کامپیوتری صورت گرفته است؛ این سوال برای پژوهشگران مطرح است که کارکنان به کدامیک از عوامل فردی و سازمانی در امنیت اطلاعات بیماران اهمیت بیشتری می‌دهند. با توجه به اینکه کارکنان مراکز بهداشت و درمان، کاربران اصلی سیستم اطلاعات بیمارستان (Hospital Information System) هستند که هدف آن بهبود کیفیت ارایه مراقبت می‌باشد و این هدف اصلی هر سازمان مراقبت بهداشتی به خصوص مؤوسسات بیمارستانی است بررسی دیدگاه کارکنان نسبت به امنیت اطلاعات سلامت ضروری به نظر می‌رسد؛ بنابراین پاسخ به این سؤال پژوهشگران را ترغیب نمود تا مطالعه‌ای با هدف شناسایی اولویت‌های کارکنان نسبت به عوامل موثر امنیت اطلاعات الکترونیکی سلامت انجام دهند.

روش بررسی

این پژوهش، از نوع توصیفی می‌باشد که جامعه پژوهش شامل ۴۰۰ نفر از کارکنان شاغل در بیمارستان‌های تابعه علوم پزشکی سمنان در سال ۹۲-۱۳۹۱ خورشیدی بود. در این مطالعه پژوهشگر روش تمام شماری (سرشماری) را به کار گرفته و نمونه‌گیری استفاده نشد. ابزار گردآوری داده‌ها پرسش‌نامه پژوهشگر ساخته بود که براساس متون علمی مربوطه، طراحی گردید. پرسش‌نامه شامل ۴ بخش و ۱۷ سؤال بود بخش اول مربوط به سؤالات دموگرافیک بود از قبیل سن، جنس، سطح تحصیلات، سابقه کار، شغل. بخش دوم حاوی ۴ سؤال در مورد عوامل موثر بر رعایت رفتارهای امنیتی بود که عواملی چون آموزش کارکنان، درک کارکنان از اهمیت امنیت اطلاعات، انگیزه و تمایل کارکنان برای مشارکت در برنامه‌های امنیت اطلاعات و مجازات و پیگردهای قانونی با متخلفین در صورت افشای اطلاعات را می‌سنجید و در بخش سوم مربوط به افراد و سازمان‌های تاثیرگذار شامل ۴ سوال بود که نقش کاربران سیستم‌های اطلاعاتی، مدیران، وزارت بهداشت، وزارت اطلاعات و فناوری اطلاعات را می‌سنجید. بخش چهارم مربوط به سایر عوامل شامل ۳ سوال که نقش عوامل اقتصادی، کنترل‌های فیزیکی و زیرساخت مناسب را می‌سنجید برای موارد بخش دوم، سوم و چهارم از پاسخ‌دهندگان خواسته شد دیدگاه خود را به ترتیب اهمیت اولویت‌بندی کنند. در انتهای پرسش‌نامه یک سوال باز طراحی گردید تا جامعه آماری به سایر عوامل تاثیرگذار در امنیت اطلاعات سلامت که در پرسش‌نامه ذکر نشده بود، اشاره کنند. برای بررسی روایی صوری و محتوایی ابزار اندازه‌گیری، پرسش‌نامه توسط صاحب‌نظران رشته مدیریت اطلاعات سلامت مورد بررسی قرار گرفت به طوری که بعضی از عبارات و جملات اصلاح شد تا جامعه آماری درک درستی از مفاهیم و سؤالات داشته باشند به طوری که ۲ گویه به دلیل هم‌پوشانی با سایر سؤالات و ۲ گویه به دلیل هم‌راستا نبودن با هدف مطالعه حذف گردید. برای سنجش پایایی ابزار اندازه‌گیری، از روش آزمون و باز آزمون استفاده شد به طوری

که پرسش‌نامه به طور تصادفی بین ۲۰ نفر از جامعه آماری توزیع گردید و سپس بعد از یک هفته پرسش‌نامه مجدداً به همان جامعه داده شد و ضریب همبستگی ۷۹/۳ بدست آمد لازم به ذکر است جامعه شرکت‌کننده در پایلوت از جامعه آماری حذف شدند. پس از کسب مجوز جهت جمع‌آوری اطلاعات و رعایت اصول اخلاقی از قبیل آگاه ساختن جامعه آماری از هدف مطالعه، توضیح درباره اینکه جامعه آماری جهت شرکت در مطالعه مختار بودند و اطلاعات هویتی آنها محرمانه باقی می‌ماند، پرسش‌نامه بین تمامی جامعه آماری توزیع گردید. در این مطالعه پژوهشگر به افرادی که پرسش‌نامه را تکمیل نمی‌کردند، دوبار به فاصله یک هفته یادآوری نمود. داده‌های گردآوری شده به کمک آزمون‌های توصیفی با استفاده از نرم‌افزار SPSS مورد تجزیه و تحلیل قرار گرفت.

یافته‌ها

۶۲/۵ درصد از جامعه آماری در مطالعه شرکت کردند به طوری که ۲۵۰ مورد از ۴۰۰ پرسش‌نامه توزیع شده عودت داده شد؛ که از این میان ۵۹/۶ درصد آن‌ها کارکنان بالینی بودند نتایج نشان داد که در بین کارکنان ۶۹/۶ درصد جامعه آماری زن و ۵۵/۲ درصد کمتر از ۳۰ سال سن داشتند. از نظر مدرک تحصیلی ۶۳/۹ درصد تحصیلات کارشناسی و ۵۴/۴ درصد کمتر از ۵ سال سابقه کار داشتند (جدول ۱).

یافته‌ها مربوط به بخش عوامل رفتاری نشان داد که ۶۰/۲ درصد آموزش ضمن خدمت، ۷۰/۴ درصد درک اهمیت امنیت اطلاعات، ۵۹ درصد افراد انگیزه و تمایل کارکنان، ۱۳/۱ مجازات‌ها و پیگردهای قانونی را به عنوان اولویت‌های اول و دوم در حوزه عوامل رفتاری موثر انتخاب کردند. در بخش عوامل سازمانی نتایج نشان داد ۵۵/۷ درصد نقش کاربران سیستم‌های اطلاعاتی، ۱۸/۵ درصد نقش مدیران، ۱۷/۳ درصد نقش وزارت بهداشت را به عنوان اولین اولویت در بین افراد و سازمان‌های تاثیرگذار انتخاب کردند. همچنین در بخش سایر عوامل یافته‌ها نشان داد ۴۷/۵ درصد وجود زیرساخت مناسب، ۳۴/۷ درصد عوامل اقتصادی و ۲۱/۸

درصد کنترل‌های فیزیکی را به عنوان مهمترین اولویت محیطی موثر انتخاب کردند (جدول ۲).

جدول ۱: خصوصیات دموگرافیک کارکنان (تعداد-۲۵۰)

درصد	تعداد	خصوصیات
۶۹/۶	۱۷۴	زن
۳۰/۴	۷۶	مرد
۵۵/۲	۱۳۸	کمتر از ۳۰ سال
۴۳/۶	۱۰۹	بین ۳۰-۵۰ سال
۱/۲	۳	بالاتر از ۵۰ سال
۵۴/۴	۱۳۶	کمتر از ۵ سال
۲۸/۴	۷۱	بین ۵-۱۵ سال
۱/۲	۴۳	بین ۱۵-۳۰ سال
۶/۵	۱۵	دیپلم
۱۳/۵	۳۱	کاردانی
۶۳/۹	۱۴۷	کارشناسی
۷	۱۶	کارشناسی ارشد
۹/۱	۲۱	دکتر
۵۹/۶	۱۴۰	بالینی
۱۵/۳	۳۶	پیراپزشکی
۲۵/۱	۵۹	اداری-مالی

جدول ۲: اولویت بندی عوامل موثر بر امنیت اطلاعات سلامت

عوامل	اولویت‌ها	اول (تعداد(درصد))	دوم (تعداد(درصد))	سوم (تعداد(درصد))	چهارم (تعداد(درصد))
عوامل رفتاری	آموزش ضمن خدمت	۳۳/۷۹	۲۷/۶۵	۳۰/۱۷۰	۹/۶۲۳
	درک اهمیت امنیت اطلاعات	۳۸/۳۹۲	۳۲/۱۷۷	۲۲/۵۵۴	۷/۱۱۷
عوامل سازمانی	انگیزه و تمایل برای مشارکت	۲۹/۱۷۱	۲۹/۹۷۳	۳۰/۳۷۴	۱۰/۷۲۶
	مجازات و پیگرد قانونی	۴/۲۱۰	۸/۹۲۱	۱۵/۲۱۳	۷۱/۷۱۷۰
	کاربران سیستم‌های اطلاعاتی	۵۵/۷۱۳۶	۱۷/۶۴۳	۹/۴۲۳	۱۷/۲۴۲
	مدیران	۱۸/۵۴۵	۵۵/۶۱۳۵	۲۱/۵۶	۴/۹۱۲
	وزارت بهداشت	۱۷/۳۴۲	۱۳/۲۳۲	۴۷/۹۱۱۶	۲۱/۵۵۲
سایر عوامل	وزارت اطلاعات و فناوری اطلاعات	۱۱/۷۲۸	۱۲/۱۲۹	۲۰/۵۴۹	۵۵/۶۱۳۳
	عوامل اقتصادی	۳۴/۷۸۳	۴۹/۵۵۰	۴۴/۸۱۰۷	-
	کنترل‌های فیزیکی	۲۱/۸۵۲	۴۲/۷۱۰۷	۳۵/۶۸۵	-
	وجود زیرساخت مناسب	۴۷/۵۱۱۵	۳۴/۷۸۴	۱۷/۸۴۳	-

بحث

در این مطالعه که با هدف شناسایی اولویت‌بندی عوامل موثر بر امنیت اطلاعات الکترونیکی سلامت در مراکز درمانی انجام شد. یافته‌ها نشان داد تقریباً نیمی از جامعه آماری زیر ساخت مناسب را به عنوان مهمترین عامل انتخاب کردند به نظر می‌رسد این دسته از افراد به تاثیر زیر ساخت‌ها در ایمن سازی فضای تبادل اطلاعات بیمارستان‌ها توجه داشتند. حیثی‌فر طی مطالعه‌ای دریافت که بخش قابل توجهی از وضعیت نامطلوب امنیت فضای تبادل اطلاعات بیمارستان‌ها، به واسطه فقدان زیرساخت مناسب می‌باشد (۱۳). از سویی دیگر مطالعات نشان می‌دهد که زیر ساخت نقش مهمی در امنیت اطلاعات دارد و همچنین زیر ساخت‌های اطلاعاتی اکثر کشورها آسیب‌پذیر می‌باشد (۵، ۱۴).

نتایج نشان داد یک چهارم جامعه آماری کنترل‌های فیزیکی را عامل تاثیرگذاری دیگری در امنیت اطلاعات سلامت می‌دانستند. احتمالاً جامعه آماری که به اشتباهات اجتناب‌ناپذیر انسانی در تبادل اطلاعات توجه داشتند. به نظر می‌رسد به منظور محافظت از مکان‌هایی که جمع‌آوری اطلاعات و پردازش آنها در آنجا انجام می‌پذیرد، استفاده از کنترل‌های فیزیکی ضروری باشد. چرا که کنترل و ایجاد محدودیت در تردد کارکنان به مکان‌های حساس، یکی از نقاط کلیدی در امنیت فیزیکی است (۱۵). مطالعه محمودزاده و رادرجی نشان داد که امنیت فیزیکی سومین عامل تاثیرگذار بر آسیب‌پذیری سیستم‌های اطلاعاتی است (۱۶).

یافته‌های این مطالعه نشان داد یک سوم از کارکنان نقش عوامل اقتصادی را در امنیت اطلاعات سلامت مهم تلقی می‌کردند ممکن است این افراد تامین امنیت اطلاعات سلامت را در سازمان‌های مراقبت سلامت پر هزینه و گران می‌دانستند چرا که مطالعات نشان می‌دهد مراکز بهداشتی و درمانی از جمله بیمارستان‌ها به عنوان بزرگترین و پرهزینه‌ترین واحدهای عملیاتی بهداشت و درمان هستند که مبالغ کلانی را در زمینه پردازش و مدیریت اطلاعات هزینه می‌کنند (۱۷، ۱۸). دانشگاه‌های علوم پزشکی به دلیل

مشکلات مالی و تشکیلاتی، اولویت داشتن درمان و به دلیل هزینه زیاد استقرار سیستم امنیت اطلاعات، به مسائل امنیتی توجه کافی نداشته و از آن غافل می‌شوند (۱۳).

نتایج مطالعه حاضر نشان داد بیش از یک سوم جامعه آماری درک و آگاهی از امنیت اطلاعات را به عنوان مهمترین اولویت برای رعایت رفتارهای امنیتی انتخاب کردند. شاید این تصور وجود داشته باشد که آگاهی از امنیت اطلاعات در افراد منجر به تغییر رفتار و تقویت رفتارهای خوب امنیتی می‌شود. به طوری که مطالعات مختلفی نشان می‌دهد اگر افراد بخواهند امنیت اطلاعات را به صورت اثر بخش تامین کنند نیاز است آنچه را که از آنها انتظار می‌رود، بهتر بدانند (۲۰، ۱۹). از سویی دیگر با افزایش آگاهی کارمندان یک سازمان از امنیت اطلاعات، رعایت اصول امنیتی به تدریج نهادینه می‌شود و این امر به تغییر فرهنگ و ارزش‌های امنیتی کمک می‌کند (۲۲، ۲۱). به طوری که Shaw طی مطالعه‌ای در سال ۲۰۰۹ میلادی دریافت که هر چه غنای اطلاعاتی بیشتر باشد فرد در سطح بالاتری از درک قرار می‌گیرد و با درک بیشتر در رفتار نیز موفقیت بیشتری کسب می‌کند (۲۳).

یافته‌ها نشان داد یک سوم جامعه آماری آموزش ضمن خدمت را به عنوان مهمترین عامل انتخاب کردند. گمان می‌رود این تفکر در بین جامعه آماری حاکم باشد که آموزش کارکنان در کاهش احتمال خطر، آسیب و صدمه به دارایی‌های سازمان نظیر اطلاعات تاثیرگذار است. شبانکاره طی مطالعه‌ای نتیجه می‌گیرد که عدم ارائه آموزش‌های مناسب و عدم آگاهی و روزآمد سازی اطلاعات موجب تحمیل هزینه‌های سنگین به سازمان می‌شود، که با آموزش مناسب بخش مهمی از مسایل مربوط به کاربران اطلاعاتی حل خواهد شد (۲۴). مطالعات نشان داده‌اند که سطح آگاهی کارمندان در خصوص امنیت سیستم‌های اطلاعاتی در حد متوسطی قرار دارد و به آموزش و توجه بیشتری نیاز است و آموزش اثربخش یکی از مکانیسم‌های قدرتمند برای کاهش خطرات امنیتی است (۲۵، ۲۲، ۱۹).

داشت (۲۲). Von Sloms دریافت که قسمت عمده‌ای از خطاها که مشکلات جدی در برنامه‌های امنیتی به وجود می‌آورد مربوط به کاربران است (۴). یافته‌ها نشان داد تعداد محدودی از افراد نقش مدیران را در امنیت اطلاعات سلامت موثر می‌دانستند. نتایج حاکی از آن است که در جامعه مورد پژوهش مسأله امنیت اطلاعات سلامت بیماران جز استراتژی‌های اصلی سازمان و مدیریت قرار نگرفته است و این مسأله روی نگرش کارکنان نسبت به نقش مدیریت در حمایت از امنیت اطلاعات بیماران تأثیر گذاشته است. کشتگری طی مطالعه‌ای دریافت تمامی تلاش‌ها در امنیت تنها زمانی به نتیجه خواهد رسید که مورد حمایت مدیریت عالی سازمان قرار گیرد (۲۹). همچنین بهرامی در سال ۹۰ در مطالعه‌ای با عنوان بهبود توسعه شاخص‌های مدیریت امنیت دریافت که مدیران سازمان احساس ناامنی مداوم ندارند و یا اطلاعات ذی‌قیمتی را در معرض تهاجم نمی‌بینند و بر همین اساس است که حمایت جدی و همه‌جانبه از پیاده‌سازی و تداوم استانداردهای امنیت ندارند (۳۰، ۳۱). لازم به ذکر است که نتیجه مطالعه حاضر باید با احتیاط تفسیر گردد چرا که اولاً مطالعه با استفاده از یک پرسش‌نامه‌ی پژوهشگر ساخته انجام شده است و به هر حال مشکلات بالقوه‌ای همانند درک ضعیف سؤالات و احتمالاً تورش پاسخ، نتایج مطالعه را تهدید می‌کند. اما با توجه به روایی و پایایی پرسشنامه تأثیر اندکی بر نتایج مطالعه داشته‌اند ثانیاً عدم مشارکت ۳۷/۵ درصد از جامعه آماری از دیگر محدودیت این مطالعه است با این وجود بعضی از نتایج این مطالعه با نتایج سایر مطالعات هم راستا بوده است به نظر می‌رسد نیاز است مطالعات جامع‌تری در این راستا انجام شود تا بتوان آن را به کل جامعه تعمیم داد.

نتیجه‌گیری

نتایج نشان داد کارکنان رعایت عوامل سازمانی، رفتاری و غیره را مهمترین اولویت‌های امنیت اطلاعات الکترونیکی سلامت در نظر داشتند و در بین عوامل سازمانی، نقش کاربران سیستم‌های اطلاعاتی را در نگهداری اطلاعات

نتایج‌ها نشان داد بیش نیمی از افراد، انگیزه و تمایل کارکنان برای مشارکت در برنامه‌های امنیت اطلاعات را در اولویت اول و دوم قرار دادند. احتمالاً این دسته از کارکنان بر این عقیده بودند هر گونه برنامه‌ای که برای سازمان طراحی می‌گردد باید متأثر از نوع تصورات، باورها، اعتقادات و ارزش‌های افراد موجود در سازمان باشد. به طوری که مطالعات نشان می‌دهد هر سازمان بنا بر فرهنگ و نظام ارزشی خود از رفتار مناسب و صحیح تعریف خاصی دارد و فرهنگ در سازمان بهداشتی - درمانی تعیین کننده‌ی مرز سازمان است و نوعی احساس هویت و تعهد به اعضای سازمان می‌دهد و عاملی در شکل دادن و به وجود آمدن رفتار کارکنان می‌باشد (۲۶، ۲۷). همچنین مطالعات مختلفی نشان می‌دهد که عوامل فرهنگی، تمایلات، باورها و عقاید بر رفتارهای امنیتی کارکنان موثر است (۸، ۲۸).

یافته‌ها این مطالعه نشان داد تعداد خیلی کمی از جامعه آماری مجازات‌ها و پیگردهای قانونی در صورت افشای اطلاعات را در رعایت اصول امنیتی مهم تلقی کردند. گمان می‌رود اکثر کارکنان که برای حفاظت از اطلاعات در سازمان، تدوین خط‌مشی‌هایی برای مجازات افرادی که تخلف می‌کنند را اثربخش نمی‌دانستند. چرا که فقدان قوانین و مقررات مکتوب باعث خواهد شد که در صورت بروز تخلف، مرجعی برای رسیدگی به تخلف وجود نداشته باشد (۱۶). به طوری که استاندارد ایزو ۲۷۰۰۷ ISC نیز بر لزوم فرایندهای انضباطی در سازمان‌های مراقبت سلامت و توجه به تخلفات در زمینه امنیت اطلاعات تأکید دارد (۱۵). از سوی دیگر محمودزاده و رادرجی دریافتند ۱۰ درصد افراد معتقد بودند با تشویق و تنبیه میتوان شرایطی را فراهم کرد تا امنیت در سازمان ارتقا یابد (۱۶). نتایج مطالعه حاضر نشان داد بیش از نیمی از جامعه آماری نقش کاربران را در امنیت سیستم‌های اطلاعاتی مهم می‌دانستند. شاید آنها رفتارهای درست و سازنده کاربران را در افزایش امنیت اطلاعات اثر بخش می‌دانستند.

kruger و kearny دریافتند بدون در نظر گرفتن نقش کاربران راه‌حل‌های فنی تأثیری در مدیریت امنیت نخواهد

راستای تعلیم نیروی انسانی کارآمد و توسعه روال‌های صحیح ضروری باشد. همچنین لازم است وزارت بهداشت به سرمایه‌گذاری بر راه‌های فنی و ایجاد زیرساخت مناسب برای بهبود امنیت اطلاعات سلامت توجه ویژه نماید.

سلامت مهمتر می‌دانستند. به نظر می‌رسد در جهت افزایش ضریب امنیت اطلاعات الکترونیکی سلامت در مراکز بهداشت و درمان ایجاد سیاست‌های کنترلی، برگزاری دوره‌های آگاه‌سازی، ترویج و توسعه برنامه‌های آموزشی دقیق در

References

1. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management* 2010; 6(4): 279-314.
2. Büyükoçkan G, Çifçi G, Gülerüz S. Strategic analysis of healthcare service quality using fuzzy AHP methodology. *Expert Systems with Applications* 2011; 38(8): 9407-24.
3. Hajrahimi N, Dehaghani SMH, Sheikhtaheri A. Health Information Security: A Case Study of Three Selected Medical Centers in Iran. *J Acta Inform Med* 2013; 21(1): 42-5.
4. Da Veiga A, Eloff JHP. A framework and assessment instrument for information security culture. *J Comput & Secur* 2010; 29(2):196-207.
5. Chung K, Wang C. Information systems resources and information security. *J Inf Syst Front* 2011; 13(4) :579-93.
6. Liu CH, Chung YF, Chen TS, Wang SD. The enhancement of security in healthcare information systems. *J Med Syst* 2012; 36(3): 1673-88.
7. Odabi OI, Oluwasegun S. Data security in health information systems by applying software techniques. *Journal of Emerging Trends in Engineering and Applied Sciences* 2011; 2(5): 775-81.
8. Rezgui Y, Marks A. Information security awareness in higher education: An exploratory study. *J Comput & Secur* 2008; 27(7): 241-253.
9. Von Solms R, Von Solms B. Information security management (1): Why information security is so important. *J Inf Manag Comput Secur* 2004; 6:174 -77.
10. Von Solms B, Von Solms R. The 10 deadly sins of information security management. *Computers & Security* 2004; 23(5), 371-6.
11. Kritzinge E, Smith E. Information security management: An information security retrieval and awareness model for industry. *J Comput & secur* 2008; 27(5):224-31.
12. Akazawa S, Igarashi M, Sawa H, Tamashiro H. Strategic Approach to Information Security and Assurance in Health Research. *Environ Health Prev Med*. 2005 Sep; 10(5): 282-5.
13. Mastaneh Z, Alipour J, Hayavi Haghghi MH. Managing health care information systems. 1th Ed. Tehran: nashre Rasool; 2010. [In Persian]
14. Habibifar V. Operational Model for Information Security. *Proceeding of the First congress of IT in Health*; 19-21 Oct 2011; Sari: Mazandaran University of Medical Sciences. [In Persian]
15. Evans k, Reeder F. A human capital crisis in cyber security: Technical Proficiency Matters. CSIS. A Report of the CSIS Commission on Cybersecurity for the 44th presidency; 2010.
16. Institute of Standards and Industrial Research of Iran. Health informatics Information security management in health using ISO/IEC 27002. [On Line]. Available from: URL: www.irannsr.org. [In Persian]
17. Mahmoodzade A, Radrajabi M. Management Security in Information System. *J Manage Sci Iran* 2007; 1(4): 78-112. [In Persian]
18. Borzekowski R. Measuring the cost impact of hospital information systems: 1987-1994. *J Health Econ* 2009; 28(5): 938-49.
19. Tabibi SJ, Farhangi AA, Nasiripour AA, Kazemzadeh RB, Ebrahimi P. Association between Harrison Cultural Typology and Acceptance of Hospital Information System. *Health Inf Manage* 2013; 10(3): 380-90. [In Persian]
20. Hasanzadeh M, Karimzadegan moghadam D, Jahangiri N. Provide a conceptual framework for evaluating the enrichment and education of information security awareness of users. *J of Syst Inf Serv* 2011; 1(2):1-16. [In Persian]
21. Aloul F A. The Need for Effective Information Security Awareness. *J Adv Inf Tech* 2012; 3(3):176-83.
22. Nikrerk JF, Solms Van. Information security culture: a management perspective. *J Comput & secur* 2009; 5: 142-4.
23. Kruger HA, Kearney WD. A prototype for assessing information security awareness. *J Comput & secur* 2006; 25:289-96.

24. Shaw RS, Chen CC, Harris AL, Huang HJ. The impact of information richness on information security awareness training effectiveness. *J Comput & Edu* 2009; 52(1): 92-100.
25. Ghasemi shabankare k, Mokhtari V, Aminilari M. security and electronic commerce. Proceeding of the 4th Ecommerce. 2007 24-25Nov, Tehran, 2007. [In Persian]
26. Eminağaoğlu M, Uçar E, Eren Ş. The positive outcomes of information security awareness training in companies—A case study. *J Inf Secur Tech Rep* 2009; 14(4): 223-9.
27. Yarmohammadian MH, Bahrami S. Organizational Culture in Health Systems. 1th Ed. Isfahan: Honarhay Ziba Publisher; 2006. [In Persian]
28. Abzari M, Yarmohammadian MH, Iravani H. Relationship between Organizational Culture and Netiquette among Academic Staff in Isfahan University of Medical Sciences (IUMS). *J Health Inf Manage* 2011; 7(4): 443. [In Persian].
29. Bulgurcu B, Cavusoglu H, Benbasat I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *J MIS quarterly* 2010; 34(3): 523-48.
30. Keshtgari M, Ghane S. Model of in the information security policy. Proceeding of the 2th international Conference on Electronic Municipality. [In Persian]
31. Bahrami M. Development and improvement of information security management Security. First congress of IT in Health; 19-21 Oct 2011; Sari: Mazandaran University of Medical Sciences. [In Persian]

The Prioritization of Effective Factors on Electronic Health Information Security in Medical Centers*

Mehdi Kahouei¹, Zainab Abbasi²

Original Article

Abstract

Introduction: The use of new technologies has created much concern about privacy and security of health information. As regards health care workers are the main users of hospital information system aiming to improve the quality of care, this study as aimed to evaluate employee's perspective towards electronic health information security.

Methods: This descriptive study was performed on 400 workers working in medical centers affiliated to Semnan University of Medical Sciences in 2012-13. Data has collected by a research made questionnaire which its validity was confirmed by experts and its reliability was justified by test-retest and analyzed by descriptive tests

Results: the findings indicated that 55.7% selected employees' role, 38.3% chose the perception of the importance of information security, 33% selected in service training and 47.5% chose proper infrastructure as the most important factors in health information security.

Conclusion: It is concluded, the employees selected organizational, behavioral and other factors as the most important factors. It seems the control policy, the training courses, the investing in technology and the appropriate infrastructures are necessary to improve electronic health information security in medical centers.

Keywords: Health Information Systems; Data Security; Academic Medical Centers.

Received: 5 Mar, 2014

Accepted: 29 Jun, 2014

Citation: Kahouei M, Abbasi Z. **The Prioritization of Effective Factors on Electronic Health Information Security in Medical Centers.** Health Inf Manage 2015; 12(2):170.

*- This article was resulted from BSc Thesis.

1- Assistant Professor, Health information management, Research Center of Social Determinant for Health, Nursing and allied health, Semnan University of Medical Sciences, Semnan, Iran

2- BSc, Health Information Technology, Student Research Committee, Semnan University of Medical Sciences, Semnan, Iran (Corresponding Author) Email: Z.abasi6516@yahoo.com