ارزیابی امنیت سیستم‌های اطلاعات بیمارستانی

زهرا میدانی[1]، محمد امین عصاری[2]، سید غلامعباس موسوی[3]، علی عطائی اندزق[4]

مقاله پژوهشی

چکیده

مقدمه: امنیت سیستم شامل مجموعه‌ای از حفاظت‌های امنیتی مرتبط با نرم‌افزار، سخت‌افزار، کارکنان و سیاست‌های سازمانی می‌باشد که از سیستم‌های اطلاعاتی در برابر تهدیدات داخلی و خارجی محافظت می‌کند. مطالعه حاضر با هدف ارزیابی امنیت سیستم‌های اطلاعات بیمارستانی HIS (Hospital Information Systems) در سه حوزه امنیت مدیریتی، فیزیکی و فنی انجام شد.

روش بررسی: این مطالعه از نوع کیفی- توصیفی و جامعه پژوهش شامل چهار بیمارستان آموزشی دولتی از مناطق مختلف کشور بود که هر کدام HIS متفاوتی داشتند. داده‌ها با استفاده از چک‌لیستی مشتمل بر ۱۳۴ سؤال جمع‌آوری گردید. به منظور طراحی چک‌لیست، ابتدا معیارهای امنیتی لازم از روی استانداردهای امنیتی شناسایی و سپس الزامات امنیت HIS با استفاده از تکنیک Delphi اصلاح شده در سه حیطه امنیت مدیریتی، فیزیکی و فنی تعیین شد. پاسخ هر یک از سؤالات چک‌لیست به صورت بله (نمره ۱) و خیر (نمره صفر) در نظر گرفته شد. سطوح امنیتی HIS نیز از صفر تا ۱۰۰ درصد و در پنج سطح خیلی پایین تا خیلی بالا تعیین گردید. داده‌ها با استفاده از آمار توصیفی مانند فراوانی و درصد مورد تجزیه و تحلیل قرار گرفت.

یافته‌ها: امنیت مدیریتی HIS در بیمارستان‌های مورد بررسی با ۳۱/۸ درصد و امنیت فیزیکی با ۲۵/۰ درصد در سطح پایینی قرار داشت. امنیت فنی HIS نیز در بیمارستان‌ها با ۴۲/۶ درصد، در سطح متوسطی بود.

نتیجه‌گیری: نتایج مطالعه حاضر با آشکار ساختن نقاط ضعف امنیت HIS، بستر مناسبی را برای مدیران بخش‌های مدیریت اطلاعات سلامت و فن‌آوری اطلاعات بیمارستان‌ها فراهم می‌آورد تا در زمینه تدوین خط‌مشی‌ها، آموزش کاربران، کنترل دسترسی، مدیریت خطر و سایر ابعاد استانداردهای مدیریتی و فیزیکی اقدامات اصلاحی مناسبی را اجرا نمایند.

واژه‌های کلیدی: امنیت؛ سیستم‌های اطلاعات بیمارستانی؛ امنیت مدیریتی

دریافت مقاله: ۱۳۹۶/۳/۱ پذیرش مقاله: ۱۳۹۶/۸/۱۷

ارجاع: میدانی زهرا، عصاری محمد امین، موسوی سید غلامعباس، عطائی اندزق علی. **ارزیابی امنیت سیستم‌های اطلاعات بیمارستانی.** مدیریت اطلاعات سلامت ۱۳۹۶؛ ۱۴ (۵): ۱۹۳-۱۸۷

مقدمه

امنیت اطلاعات از این جهت که از سیستم‌های اطلاعاتی در برابر تهدیدات داخلی و خارجی محافظت می‌کند، موضوع مهمی است. در واقع، سرنوشت یک سازمان به سطوح فن‌آوری اطلاعات و حفاظت اطلاعات آن سازمان وابسته می‌باشد (۱). حفاظت از تجهیزات کامپیوتری، داده، اطلاعات و خدمات کامپیوتری در برابر دسترسی‌های ناخواسته و غیر مجاز، حوادث غیر مترقبه و تخریب‌های فیزیکی، برای هر فرد یا سازمانی که از کامپیوتر استفاده می‌کند، امری حیاتی است (۲). امنیت اطلاعات بخشی از اصول سه‌گانه محرمانگی، یکپارچگی و قابلیت دسترسی می‌باشد. محرمانگی تضمین می‌کند که فقط افراد مجاز حق دسترسی به اطلاعات دارند. قابلیت دسترسی تضمین می‌کند که افراد مجاز در مواقع نیاز می‌توانند به اطلاعات دسترسی داشته باشند. یکپارچگی نیز تضمین می‌کند که اطلاعات به روش غیر مجاز در معرض تغییر و تخریب قرار نمی‌گیرد (۳).

تهدیدات امنیتی سیستم‌های اطلاعات مراقبت سلامت در سال‌های اخیر به صورت چشمگیری افزایش یافته است (۴). نتایج مطالعه Fernando و Dawson در خصوص امنیت داده و محرمانگی بالینی نشان داد که امنیت سیستم‌های اطلاعات سلامت آسیب‌پذیر می‌باشد (۵). این در حالی است که حفظ محرمانگی و رازداری اطلاعات، یکی از نگرانی‌های عمده بیماران محسوب می‌شود. نتایج تحقیقی در آمریکا حاکی از آن بود که ۷۵ درصد بیماران نگران افشای غیر مجاز اطلاعات محرمانه‌شان و به اشتراک گذاشته شدن آن‌ها در وب‌سایت‌ها هستند (۶). یافته‌های پژوهشی در اسپانیا نشان داد که ۶۲ درصد کاربران سیستم‌های

مقاله حاصل طرح تحقیقاتی با شماره ۹۳۱۰۳ می‌باشد که با حمایت دانشگاه علوم پزشکی کاشان انجام شده است.

۱- دانشیار، مدیریت اطلاعات سلامت، مرکز تحقیقات مدیریت اطلاعات سلامت و گروه مدیریت و فن‌آوری اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی کاشان، کاشان، ایران

۲- مربی، مهندسی کامپیوتر، گروه مهندسی کامپیوتر و فن‌آوری اطلاعات، دانشگاه پیام نور، تهران، ایران

۳- مربی، آمار و اپیدمیولوژی، گروه آمار، دانشکده بهداشت، دانشگاه علوم پزشکی کاشان، کاشان، ایران

۴- کارشناس ارشد، فن‌آوری اطلاعات سلامت، گروه مدیریت و فن‌آوری اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی کاشان، کاشان، ایران (نویسنده مسؤول)

Email: ali.ataie_meshgini@yahoo.com

اطلاعاتی، پسورد ضعیفی انتخاب کرده‌اند (۷). در مطالعه دیگری که در کانادا صورت گرفت، پژوهشگران قادر به شکستن پسورد ۹۳ درصد فایل‌ها شدند. همچنین، مشخص شد که فایل‌های محتوای اطلاعات سلامت شخصی بیماران به وسیله ایمیل و درایوها به اشتراک گذاشته می‌شود (۸). شریفیان و همکاران در پژوهش خود به این نتیجه رسیدند که رویه خاتمه دسترسی در هیچ یک از بیمارستان‌های مورد مطالعه اجرا نمی‌شود و باید فرایندی برای خاتمه دسترسی به اطلاعات الکترونیکی حفاظت شده هنگامی که یک عضو نیروی کار مدت زمان زیادی وجود نداشته است، به کار گرفته شود (۹).

سازمان‌های مختلف دولتی و خصوصی، استانداردها، معیارها و دستورالعمل‌های قانونی گوناگونی را به منظور پشتیبانی و تأمین سطوح امنیت اطلاعات طراحی کرده‌اند (۱۰). به عنوان مثال، استاندارد بین‌المللی ISO ۲۷۰۰۱، الزامات و کنترل‌هایی برای ایجاد، پیاده‌سازی، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات و استاندارد امنیتی قانون قابلیت انتقال و مسؤولیت‌پذیری بیمه سلامت HIPAA (Health Insurance Portability And Accountability Act) نیز مکانیسم‌های مدیریتی، فیزیکی و فنی را در راستای حفاظت از اطلاعات الکترونیکی سلامت ارایه نموده است (۱۱). کنترل امنیت مدیریتی عبارت است از «اقدامات، سیاست‌ها و رویه‌های مدیریتی جهت حفاظت از اطلاعات سلامت الکترونیکی». کنترل امنیت فیزیکی شامل حفاظت از سخت‌افزار، نرم‌افزار، داده‌ها و اطلاعات کامپیوتر در برابر آسیب‌های فیزیکی است. منظور از امنیت فنی، روش‌های فنی جهت تضمین امنیت اطلاعات سلامت می‌باشد (۱۲).

از آن‌جا که سازمان‌های مختلف دارای اندازه، ویژگی‌ها و فرایندهای کاری متفاوتی هستند و استانداردهای مختلف امنیتی همچون HIPAA، ISO و سایر قوانین امنیتی، ابعاد مختلفی از امنیت اطلاعات را پوشش می‌دهد، استفاده از یک معیار جهت ارزیابی امنیت اطلاعات آن سازمان‌ها کافی نیست و باید ترکیبی از معیارهای مختلف استفاده گردد (۱). مطالعات صورت گرفته در ایران نشان می‌دهد که ایمنی اطلاعات پرونده الکترونیک سلامت، یکی از ضروریات حرکت به سمت ایجاد استفاده از پرونده‌های الکترونیک سلامت در هر کشوری است و کشور ما فاقد الزامات جامعی در این زمینه می‌باشد (۱۳).

با توجه به رویکرد کشور به سمت پرونده الکترونیک سلامت و لزوم حفاظت از اطلاعات سلامت بیماران، بررسی وضعیت امنیت سیستم‌های اطلاعات بیمارستان HIS (Hospital Information Systems) از اهمیت خاصی برخوردار است. مطالعه حاضر با هدف ارزیابی امنیت HIS در سه حوزه کنترل‌های امنیت مدیریتی، فیزیکی و فنی با استفاده از استانداردهای امنیتی معتبر انجام شد تا گامی در جهت تقویت امنیت HIS بردارد.

روش بررسی

این پژوهش از نوع کیفی- توصیفی بود که در اسفند سال ۱۳۹۳ و بهار سال ۱۳۹۴ انجام گردید. ابزار جمع‌آوری داده‌ها، چک‌لیستی متشکل از ۱۳۴ سؤال در سه حیطه امنیت مدیریتی (۴۰ الزام)، امنیت فیزیکی (۱۹ الزام) و امنیت فنی (۷۵ الزام) بود که با استفاده از تکنیک Delphi اصلاح شده تهیه شد. بدین صورت که ابتدا معیارهای امنیتی موجود در استانداردهای HIPAA، ISO ۲۷۰۰۱ و مؤسسه پرونده کامپیوترمحور بیمار CPRI (Computer-Based Patient Record Institute) به علت فراهم کردن معیارهای امنیتی جهت ارزیابی و پژوهش‌های آینده و نیز وجود تحقیقات و ارزیابی‌های مختلف مطابق با این معیارها، به عنوان ابزار ارزیابی مورد استفاده قرار گرفت. بر اساس مطالعات انجام شده، استاندارد HIPAA یکی از پرکاربردترین استانداردها جهت حفظ محرمانگی و امنیت اطلاعات سلامت محسوب می‌شود. ISO ۲۷۰۰۱ نیز از دیگر استانداردهای مهم در حوزه امنیت اطلاعات به شمار می‌رود (۱۴).

در مرحله بعد، معیارهای مربوط به صورت مجزا از روی استانداردهای امنیتی مذکور، استخراج و چک‌لیست‌های سه استاندارد با هم تلفیق شد. موارد مشابه حذف گردید و تمام موارد متفاوت در هر یک از محورهای مذکور، در الگوی اولیه گنجانده شد. برای رسیدن به اجماع در خصوص هر یک از معیارها در بین خبرگان، تکنیک Delphi اصلاح شده مورد استفاده قرار گرفت. این تکنیک یکی از انواع تکنیک Delphi و روش اجرای آن مانند Delphi کلاسیک می‌باشد که برای رسیدن به اجماع بین خبرگان تا حصول نتایج در چندین فاز اجرا می‌شود. با این تفاوت که به جای فاز اول، اغلب از جلسه گروه متمرکز استفاده می‌گردد (۱۵). به منظور اجرای جلسات گروه متمرکز، ابتدا تیمی شامل یک نفر از استادان به عنوان گرداننده بحث و دبیر جلسه و یک نفر به عنوان یادداشت‌بردار جهت یادداشت‌برداری و ضبط مکالمات، انتخاب گردید. جلسات گروه متمرکز در ۶ جلسه و با حضور ۶ نفر از متخصصان شامل دو نفر دکتری مدیریت اطلاعات بهداشتی، دو نفر دانشجوی دکتری فن‌آوری اطلاعات، یک نفر کارشناس ارشد مهندسی کامپیوتر و یک نفر کارشناس ارشد امنیت شبکه، در لابراتوار دانشگاه علوم پزشکی کاشان تشکیل شد. لازم به ذکر است که شرکت کنندگان از بین افرادی که در حوزه امنیت سیستم‌های اطلاعاتی تجربه، تدریس و یا پژوهش داشتند، انتخاب گردید. در این جلسات تمامی الزامات تعیین شده به بحث و بررسی گذاشته شد. جهت استفاده بهتر از نظرات شرکت کنندگان، بعد از اتمام جلسات، مطالب یادداشت‌برداری و ضبط شده در طول جلسه مورد بررسی و تحلیل قرار گرفت.

برای تعیین توافق بر روی الزامات اصلی، تمامی الزامات در قالب پرسش‌نامه بر اساس تکنیک Delphi به رأی ۳۰ نفر از متخصصان (با همان شرایط ذکر شده برای جلسات گروه متمرکز) گذاشته شد. برای قضاوت در خصوص پذیرش یا رد هر یک از آیتم‌ها، از مجموع امتیاز استفاده شد؛ بدین صورت که مواردی که کمتر از ۵۰ درصد صاحب‌نظران تأیید کردند، حذف گردید و مواردی که ۷۵ درصد و بیشتر تأیید نمودند، مورد قبول قرار گرفت. همچنین، مواردی که بین ۵۰ تا ۷۵ درصد مورد تأیید بود، مجدد به نظرخواهی گذاشته شد. اعتبار علمی چک‌لیست تحت نظر استادان راهنما و مشاور و طبق شاخص روایی محتوا و نسبت روایی محتوا و با استفاده از نظر ۱۰ نفر از متخصصان مدیریت اطلاعات بهداشتی، متخصصان فن‌آوری اطلاعات و متخصصان رشته‌های کامپیوتری و شبکه تعیین شد که روایی تمامی سؤالات با مقدار بیشتر از ۰/۸ مورد پذیرش قرار گرفت.

به دلیل اعمال محدودیت‌هایی از سوی بیمارستان‌ها مبنی بر محرمانگی اطلاعات و عدم همکاری بیمارستان‌ها در برخی پژوهش‌ها، توافق شد بیمارستان‌هایی انتخاب شوند که امکان هماهنگی و دسترسی آسان به HIS آن‌ها میسر باشد. به همین دلیل، چهار بیمارستان آموزشی دولتی شامل بیمارستان کودکان تبریز، امام رضا (ع) مشهد، رازی تهران و شهید بهشتی کاشان که هر کدام دارای HIS متفاوتی بودند، به عنوان جامعه پژوهش انتخاب شدند. به دلیل این که شرکت‌های تأمین کننده HIS هر یک از بیمارستان‌های

جدول ۱: وضعیت امنیت مدیریتی سیستم اطلاعات بیمارستانی

استانداردهای امنیت مدیریتی	تعداد کل الزامات	بهشتی تعداد (درصد)	رازی تعداد (درصد)	کودکان تعداد (درصد)	امام رضا (ع) تعداد (درصد)	کل تعداد (درصد)
خط‌مشی امنیتی	۷	۰ (۰)	۰ (۰)	۰ (۰)	۰ (۰)	۰ (۰)
مسؤولیت امنیت اطلاعات	۶	۲ (۳۳/۳)	۱ (۱۶/۶)	۱ (۱۶/۶)	۳ (۵۰/۰)	۱/۷ (۲۹/۱)
امنیت منابع انسانی	۱۰	۵ (۵۰/۰)	۴ (۴۰/۰)	۳ (۳۰/۰)	۴ (۴۰/۰)	۴ (۴۰/۰)
مدیریت دسترسی به اطلاعات	۸	۳ (۳۷/۵)	۲ (۲۵/۰)	۳ (۳۷/۵)	۴ (۵۰/۰)	۳ (۳۷/۵)
حوادث امنیتی	۶	۳ (۵۰/۰)	۳ (۵۰/۰)	۳ (۵۰/۰)	۳ (۵۰/۰)	۳ (۵۰/۰)
قراردادهای مرتبط با کسب و کار	۳	۱ (۳۳/۳)	۱ (۳۳/۳)	۱ (۳۳/۳)	۱ (۳۳/۳)	۱ (۳۳/۳)
مجموع	۴۰	۱۴ (۳۵/۰)	۱۱ (۲۷/۵)	۱۱ (۲۷/۵)	۱۵ (۳۷/۵)	۱۲/۷ (۳۱/۸)

مورد بررسی تفاوت داشتند و بیمارستان‌ها از مناطق مختلف کشور انتخاب شدند، امکان تعمیم کشوری بیشتر بود. اطلاعات مربوط به هر الزام، توسط پژوهشگر و از طریق مشاهده HIS، مشاهده مستندات و مصاحبه با مسؤولان فن‌آوری اطلاعات جمع‌آوری گردید. پاسخ هر یک از سؤالات چک‌لیست به صورت بله (نمره یک) و خیر (نمره صفر) در نظر گرفته شد. بدین ترتیب که در صورت وجود و رعایت الزام موجود در چک‌لیست در سیستم، نمره بله (۱) و در صورت عدم وجود یا عدم رعایت الزام، نمره خیر (صفر) اختصاص یافت. سطوح امنیتی نیز در پنج سطح شامل خیلی پایین (۱۹/۹۹-۰)، پایین (۳۹/۹۹-۲۰)، متوسط (۵۹/۹۹-۴۰)، بالا (۷۹/۹۹-۶۰) و خیلی بالا (۱۰۰-۸۰) تعیین شد. در نهایت، داده‌ها با استفاده از آمار توصیفی مانند فراوانی و درصد در نرم‌افزار SPSS نسخه ۲۲ (version 22, IBM Corporation, Armonk, NY) مورد تجزیه و تحلیل قرار گرفت.

یافته‌ها

یافته‌های به دست آمده در سه حیطه مورد بررسی نشان داد که امنیت مدیریتی HIS با ۳۱/۸ درصد و امنیت فیزیکی با ۲۵/۰ درصد در سطح پایینی قرار داشت. امنیت فنی HIS نیز با ۴۲/۶ درصد، سطح متوسطی داشت.

با توجه به جدول ۱، الزامات «خط‌مشی امنیتی» در تمام بیمارستان‌های مورد بررسی در سطح امنیتی خیلی پایینی قرار داشت. در خصوص الزامات «مسؤولیت امنیت اطلاعات» و «مدیریت دسترسی به اطلاعات» نیز بیمارستان‌ها سطح امنیتی پایینی را کسب کردند و بیمارستان امام رضا (ع) با لحاظ کردن بیشترین الزامات، در سطح متوسط قرار داشت. در خصوص الزامات «امنیت منابع انسانی»، بیمارستان‌ها در سطح امنیتی متوسطی قرار گرفتند و بیمارستان بهشتی با لحاظ کردن بیشترین الزامات، در سطح متوسط قرار داشت. در مجموع، الزامات «حوادث امنیتی» سطح امنیتی متوسط و الزامات «قراردادهای مرتبط با کسب و کار» نیز سطح امنیتی پایینی را به دست آورد. در مجموع، امنیت مدیریتی HIS در بیمارستان‌های مورد مطالعه، سطح امنیتی پایینی را به خود اختصاص داد.

با توجه به داده‌های جدول ۲، در خصوص الزامات «کنترل دسترسی به تسهیلات»، بیمارستان‌های مورد بررسی در سطح امنیتی خیلی پایینی قرار داشتند و بیمارستان امام رضا (ع) با لحاظ کردن بیشترین الزامات، سطح امنیتی پایینی را به دست آورد. در خصوص الزامات «کنترل وسیله و رسانه» نیز بیمارستان‌ها در سطح امنیتی متوسطی قرار گرفتند که بیمارستان امام رضا (ع) با لحاظ کردن بیشترین الزامات و بیمارستان رازی نیز با لحاظ کردن کمترین الزامات، به ترتیب سطح متوسط و پایینی داشتند. در مجموع، امنیت فیزیکی HIS در بیمارستان‌های مورد مطالعه، در سطح امنیتی پایینی قرار داشت.

با توجه به داده‌های حاصل از جدول ۳، در خصوص الزامات «کنترل دسترسی» و «کنترل ممیزی»، بیمارستان‌های مورد بررسی در سطح امنیتی متوسطی قرار داشتند که بیمارستان امام رضا (ع) با لحاظ کردن بیشترین الزامات، سطح امنیتی متوسطی را به دست آورد. در خصوص الزامات «یکپارچگی»، همه بیمارستان‌ها سطح امنیتی متوسطی را کسب کردند. در خصوص الزامات «امنیت ذخیره و انتقال داده» نیز بیمارستان‌ها در سطح امنیتی پایینی قرار داشتند و بیمارستان بهشتی با لحاظ کردن بیشترین الزامات در سطح متوسطی بود. در مجموع، امنیت فنی HIS در بیمارستان‌های مورد مطالعه، در سطح امنیتی متوسطی قرار داشت.

جدول ۲: وضعیت امنیت فیزیکی سیستم اطلاعات بیمارستانی

استانداردهای امنیت فیزیکی	تعداد کل الزامات	بهشتی تعداد (درصد)	رازی تعداد (درصد)	کودکان تعداد (درصد)	امام رضا (ع) تعداد (درصد)	کل تعداد (درصد)
کنترل دسترسی به تسهیلات	۱۴	۲ (۱۴/۲)	۲ (۱۴/۲)	۳ (۲۱/۴)	۴ (۲۸/۵)	۳ (۱۹/۵)
کنترل وسیله و رسانه	۵	۲ (۴۰/۰)	۱ (۲۰/۰)	۲ (۴۰/۰)	۳ (۶۰/۰)	۲ (۴۰/۰)
مجموع	۱۹	۴ (۲۱/۵)	۳ (۱۵/۷)	۵ (۲۶/۳)	۷ (۳۶/۸)	۵ (۲۵/۰)

جدول ۳: وضعیت امنیت فنی سیستم اطلاعات بیمارستانی

استانداردهای امنیت فنی	تعداد کل الزامات	بهشتی تعداد (درصد)	رازی تعداد (درصد)	کودکان تعداد (درصد)	امام رضا (ع) تعداد (درصد)	کل تعداد (درصد)
کنترل دسترسی	۴۲	۱۸ (۴۲/۸)	۱۷ (۴۰/۴)	۱۴ (۳۳/۳)	۱۹ (۴۵/۲)	۱۷ (۴۰/۴)
کنترل ممیزی	۱۶	۸ (۵۰/۰)	۶ (۳۷/۵)	۷ (۴۳/۷)	۹ (۲/۵۶)	۷/۵ (۴۶/۸)
یکپارچگی	۸	۴ (۵۰/۰)	۴ (۵۰/۰)	۴ (۵۰/۰)	۴ (۵۰/۰)	۴ (۵۰/۰)
امنیت ذخیره و انتقال داده	۹	۵ (۵۵/۵)	۳ (۳۳/۳)	۲ (۲۲/۲)	۴ (۴۴/۴)	۳/۵ (۳۸/۸)
مجموع	۷۵	۳۵ (۴۶/۶)	۳۰ (۴۰/۰)	۲۷ (۲۶/۰)	۳۶ (۴۸/۰)	۳۲ (۴۲/۶)

بحث

یافته‌های مطالعه حاضر نشان داد که در بیمارستان‌های مورد بررسی، امنیت مدیریتی و امنیت فیزیکی در سطح پایین و امنیت فنی در سطح متوسطی قرار داشت.

امنیت مدیریتی: بر اساس یافته‌های به دست آمده، الزامات «خط‌مشی امنیتی» در بیمارستان‌های مورد مطالعه در سطح امنیتی خیلی پایینی قرار داشت که با نتایج سایر پژوهش‌ها (۱۱، ۹) همسو نبود. نتایج تحقیق Park و همکاران نشان داد که ۶۰ درصد بیمارستان‌ها دارای سند خط‌مشی امنیت اطلاعات هستند و در ۳۵/۶ درصد بیمارستان‌ها، بازنگری دوره‌ای خط‌مشی‌های امنیتی انجام می‌شود (۱۱). در همین راستا، نتایج مطالعه شریفیان و همکاران حاکی از آن بود که آزمایش و تجدید نظر رویه‌ها در نیمی از بیمارستان‌ها اعمال می‌گردد (۹). تدوین یک سند خط‌مشی جامع امنیت اطلاعات توسط مدیریت و ابلاغ و اطلاع‌رسانی آن به کارکنان و همچنین، بازنگری دوره‌ای این سند می‌تواند موجب بهبود امنیت اطلاعات سلامت سازمان شود.

بر اساس نتایج پژوهش حاضر، الزامات «مسؤولیت امنیت اطلاعات» در سطح پایینی قرار داشت که با نتایج سایر مطالعات (۹، ۱) مشابه بود. نتایج پژوهش Jo و همکاران نشان داد که در بیمارستان‌های مورد مطالعه، نقش‌ها و مسؤولیت‌های امنیت اطلاعات به صورت واضح مشخص نشده است (۱). شریفیان و همکاران نیز به این نتیجه رسیدند که پاسخگویی امنیتی فقط در نیمی از بیمارستان‌ها اعمال می‌شود (۹). علت پایین بودن سطح امنیتی الزامات «مسؤولیت امنیت اطلاعات» در ایران را می‌توان به عدم سازماندهی یک تیم امنیتی با نقش‌ها و مسؤولیت‌های امنیتی مشخص در ایران نسبت داد.

در تحقیق حاضر، الزامات «امنیت منابع انسانی» نیز در سطح متوسطی قرار داشت. نتایج مطالعه Park و همکاران حاکی از آن بود که امنیت منابع انسانی به طور میانگین با ۶۱/۸ درصد در بیمارستان‌ها اعمال می‌شود (۱۱). شریفیان و همکاران دریافتند که امنیت نیروی کار در بیشتر بیمارستان‌ها اعمال می‌گردد (۹). در همین راستا، بیمارستان‌ها باید یک برنامه مدون آموزشی ضمن خدمت جهت یادآوری خط‌مشی‌ها و قوانین امنیتی و توانمندسازی کاربران HIS تدوین و اجرا نمایند.

بر اساس نتایج پژوهش حاضر، «مدیریت دسترسی به اطلاعات» در سطح پایینی قرار گرفت که با نتایج سایر مطالعات (۸، ۷) مطابقت داشت. نتایج مطالعه‌ای در اسپانیا نشان داد که ۶۲ درصد کاربران سیستم‌های اطلاعاتی، پسورد ضعیفی انتخاب کرده‌اند (۷). تحقیق دیگری بر روی اطلاعات سلامت شخصی بیماران در آزمایشگاه‌های بالینی در کانادا حاکی از آن بود که پسورد ۹۳ درصد از فایل‌ها قابل دستیابی می‌باشد (۸). در همین راستا، به کارگیری تدابیری در خصوص ایجاد، تغییر و حذف حق دسترسی کاربر در راستای تضمین دسترسی به اطلاعات سلامت، الزامی است.

بر اساس نتایج پژوهش حاضر، الزامات «حوادث امنیتی» در سطح متوسطی قرار داشت. بررسی‌های انجام شده در خصوص گزارش‌دهی خطاهای امنیتی سیستم‌های اطلاعات سلامت نشان داد که در هر دو کشور ایالات متحده آمریکا و کانادا، مکانیزم و یا خط‌مشی استانداردی در خصوص گزارش‌دهی و پیگیری خطاهای امنیتی وجود ندارد (۱۶). بنابراین، تدوین خط‌مشی‌هایی جهت گزارش‌دهی خطاهای امنیتی و نیز برنامه‌ریزی‌های مدیریتی جهت شناسایی حوادث امنیتی و نیز الزام کاربران جهت گزارش‌دهی به موقع حوادث امنیتی، می‌تواند در کاهش خطاهای امنیتی کارساز باشد (۱).

امنیت فیزیکی: نتایج مطالعه حاضر نشان داد که الزامات «کنترل دسترسی به تسهیلات» در سطح خیلی پایینی قرار داشت که با نتایج سایر تحقیقات (۱۷، ۹، ۴) همسو بود. شریفیان و همکاران در پژوهش خود نتیجه‌گیری کردند که طرح امنیت فیزیکی مؤسسه، فقط در یکی از بیمارستان‌ها اعمال می‌شود و نیاز به تقویت دارد (۹). نتایج مطالعه Samy و همکاران نشان داد که قطعی یا نقص برق، مهم‌ترین تهدید HIS به شمار می‌رود که علت آن نقص برق Server، نقص سیستم تهویه Server و نیز نقص و یا قطعی برق در نتیجه عملکرد نادرست کارکنان فنی واحد برق و کامپیوتر بود (۴). سیستم‌های قفل و کلید در بیش از ۹۰ درصد مؤسسات مراقبت سلامت ناکافی است که این امر علاوه بر به کارگیری سخت‌افزار نامناسب، در نتیجه ضعف مدیریتی نیز می‌باشد (۱۷). در همین زمینه، بیمارستان‌ها باید تدابیری را در خصوص کنترل فیزیکی تسهیلات، ایجاد حصارهای امنیتی برای نواحی حاوی اطلاعات، به کارگیری حفاظت فیزیکی برای مقابله با خسارت‌های انسانی و بلایای طبیعی و درگیری‌های احتمالی و همچنین، قرار دادن تجهیزات کامپیوتری در مکان مناسب به کار گیرند.

بر اساس نتایج بررسی حاضر، الزامات «کنترل وسیله و رسانه» سطح متوسطی داشت که با نتایج سایر پژوهش‌ها (۱۱، ۹) مشابه بود. یافته‌های تحقیق Park و همکاران نشان داد که تجهیزات دارای اطلاعات سلامت شخصی دور انداخته می‌شوند و به طور نامناسب استفاده مجدد می‌شوند (۱۱). شریفیان و همکاران نیز به این نتیجه رسیدند که قوانین استفاده مجدد از رسانه‌ها در اغلب بیمارستان‌ها اعمال می‌گردد (۹). با این وجود، در خصوص استفاده مجدد از رسانه‌ها در بیمارستان‌های ایران، نیاز به دقت و کنترل بیشتری می‌باشد. در همین راستا، تدوین دستورالعملی در خصوص مدت زمان نگهداری داده‌های الکترونیکی و نحوه انهدام آن‌ها و عدم استفاده مجدد از رسانه‌ها و تجهیزات الکترونیکی ضروری به نظر می‌رسد.

امنیت فنی: نتایج مطالعه حاضر حاکی از آن بود که الزامات مربوط به «کنترل دسترسی» در بیمارستان‌های مورد بررسی سطح متوسطی را کسب کرد که با نتایج سایر تحقیقات (۱۸، ۷) همخوانی داشت. نتایج پژوهشی در اسپانیا نشان داد که ۶۲ درصد کاربران سیستم‌های اطلاعاتی پسورد ضعیفی انتخاب کرده‌اند. همچنین، پسورد ۵۳/۹ درصد کاربران فاقد ترکیبی از حداقل ۸ کاراکتر شامل حروف بزرگ الفبایی، حروف کوچک الفبایی، اعداد و کاراکترهای مخصوص بود (۷). مطالعه Kruger و همکاران به این نتیجه دست یافت که استانداردهای لازم در خصوص کنترل دسترسی به سیستم‌های اطلاعاتی رعایت نشده است (۱۸).

الزامات مربوط به «رد ممیزی» سطح متوسطی را به دست آورد. نتایج پژوهش شریفیان و همکاران نشان داد که کنترل ممیزی در بیشتر بیمارستان‌ها اعمال می‌شود (۹) که با یافته‌های بررسی حاضر مطابقت داشت. با این وجود، این امر کافی نیست و باید نظارت‌های منظم بر روی کنترل ممیزی و ثبت دقیق اطلاعات در بیمارستان‌های ایران انجام گیرد. نتایج تحقیق Cruz-Correia و همکاران حاکی از آن بود که ساختار رد ممیزی موجود، کیفیت کافی جهت تضمین قابلیت ردیابی در توسعه HIS را ندارد. آن‌ها ضعیف بودن رد ممیزی را ناشی از عدم توجه مدیران ارشد اطلاعات و عدم استفاده از استانداردهای بین‌المللی در مؤسسات مراقبت سلامت پرتغال دانستند (۱۹).

الزامات مربوط به «یکپارچگی» در سطح متوسطی قرار داشت. بر اساس نتایج پژوهش شریفیان و همکاران، یکپارچگی در هیچ یک از بیمارستان‌ها اعمال نمی‌شود و این یافته نشان دهنده آن است که کنترل‌های لازم جهت حفاظت از یکپارچگی اطلاعات انجام نمی‌گیرد و باید تدابیر و سیاست‌هایی جهت حفاظت از اطلاعات در برابر تغییرات و تخریب‌های غیر مجاز به کار گرفته شود (۹).

الزامات مربوط به «امنیت ذخیره و انتقال داده» سطح پایینی را به خود اختصاص داد. مطالعه انجام شده در بیمارستان‌های اسپانیا نیز حاکی از آن بود که ۵۱/۱ درصد کاربران از رویه‌های موجود در بیمارستان جهت امحای صحیح اطلاعات محرمانه استفاده نمی‌کنند (۷). تحقیق دیگری در بیمارستان‌های نروژ نشان داد که از بین تهدیدات وارد شده به جنبه‌های چهارگانه امنیت اطلاعات (شامل محرمانگی، یکپارچگی، قابلیت دسترسی و کیفیت)، تهدیدات مربوط به محرمانگی جدی‌ترین تهدید تلقی می‌شود (۲۰). به کارگیری اقدامات لازم جهت تضمین امنیت ذخیره و انتقال اطلاعات الکترونیکی، طبقه‌بندی اطلاعات با توجه به ارزش قانونی، حساسیت و بحرانی بودن برای سازمان و همچنین، به کارگیری تدابیر فنی لازم برای تصدیق شخص یا موجودیت تقاضا کننده دسترسی به اطلاعات الکترونیکی قبل از اجازه دسترسی به اطلاعات توصیه می‌شود.

عدم همکاری به موقع برخی از مدیران و کارکنان بیمارستان‌ها در جمع‌آوری اطلاعات در طی انجام پژوهش و اعمال محدودیت از طرف مدیران به دلیل ترس از نتایج پژوهش، از جمله محدودیت‌های مطالعه حاضر بود..

نتیجه‌گیری

در مجموع، یافته‌های تحقیق حاضر نشان داد که امنیت HIS در بیمارستان‌های مورد بررسی از سطح امنیتی پایینی برخوردار می‌باشد. ضعف این سیستم‌ها در حوزه استانداردهای مدیریتی و فیزیکی تأیید کننده این مطلب است که برای تأمین امنیت HIS علاوه بر تأکید بر جنبه‌های فنی و زیرساخت فن‌آوری اطلاعات، ضروری است امنیت اطلاعات پزشکی نیز مد نظر قرار گیرد. نتایج به دست آمده از مطالعه حاضر با آشکار ساختن نقاط ضعف امنیت HIS، بستر مناسبی را برای مدیران بخش‌های مدیریت اطلاعات سلامت و فن‌آوری اطلاعات بیمارستان‌ها فراهم می‌آورد تا در زمینه تدوین خط‌مشی‌ها، آموزش کاربران، کنترل دسترسی، مدیریت خطر و سایر ابعاد استانداردهای مدیریتی و فیزیکی، اقدامات اصلاحی مناسبی را اجرا نمایند.

پیشنهادها

با توجه به این که تحقق امنیت HIS، یکی از نگرانی‌های عمده محسوب می‌شود، ضروری است تا با تقویت استانداردهای سه حوزه امنیت مدیریتی، فیزیکی و فنی، زمینه لازم برای توسعه استفاده این ابزار در سطح وسیع فراهم گردد.

تشکر و قدردانی

بدین وسیله از کلیه افرادی که در انجام این پژوهش همکاری نمودند، تشکر و قدردانی به عمل می‌آید.

References

1. Jo H, Kim S, Won D. Advanced information security management evaluation system. KSII T Internet Info 2011; 5(6): 1192-213.
2. Cucoranu IC, Parwani AV, West AJ, Romero-Lauro G, Nauman K, Carter AB, et al. Privacy and security of patient data in the pathology laboratory. J Pathol Inform 2013; 4: 4.
3. Barham C. Confidentiality and security of information. Anaesth Crit Care Med 2014; 15(1): 46-8.
4. Samy GN, Ahmad R, Ismail Z. Threats to health information security. Proceedings of the 50th International Conference on Information Assurance and Security; 2009 Aug. 18-20; Xi'An China, China.
5. Fernando JI, Dawson LL. The health information system security threat lifecycle: An informatics theory. Int J Med Inform 2009; 78(12): 815-26.
6. Appari A, Eric Johnson M. Information security and privacy in healthcare: Current state of research. International Journal Internet and Enterprise Management 2010; 6(4): 279-314.
7. Fernandez-Aleman JL, Sanchez-Henarejos A, Toval A, Sanchez-Garcia AB, Hernandez-Hernandez I, Fernandez-Luque L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. Int J Med Inform 2015; 84(6): 454-67.
8. El Emam K, Moreau K, Jonker E. How strong are passwords used to protect personal health information in clinical trials? J Med Internet Res 2011; 13(1): e18.
9. Sharifian R, Nematollahi M, Monem H, Ebrahimi F. Evaluating the security safeguards in hospital information system

according to the health insurance portability and accountability act of university hospitals in shiraz university of medical sciences. Health Inf Manage 2013; 10(1): 1-12. [In Persian].
10. Susanto H, Almunawar MN, Tuan YC. Information security management system standards: A comparative study of the big five. International Journal of Electrical & Computer Sciences 2011; 12(1).
11. Park WS, Seo SW, Son SS, Lee MJ, Kim SH, Choi EM, et al. Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. Healthc Inform Res 2010; 16(2): 89-99.
12. Karasz HN, Eiden A, Bogan S. Text messaging to communicate with public health audiences: How the HIPAA Security Rule affects practice. Am J Public Health 2013; 103(4): 617-22.
13. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security requirements and solutions in electronic health records: Lessons learned from a comparative study. J Med Syst 2010; 34(4): 629-42.
14. Fernandez-Aleman JL, Senor IC, Lozoya PA, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform 2013; 46(3): 541-62.
15. Tracy SJ. Qualitative research methods: Collecting evidence, crafting analysis, communicating impact. New York, NY: John Wiley & Sons; 2012.
16. Kushniruk AW, Bates DW, Bainbridge M, Househ MS, Borycki EM. National efforts to improve health information system safety in Canada, the United States of America and England. Int J Med Inform 2013; 82(5): e149-e160.
17. York TW, MacAlister D. Physical security safeguards. In: York TW, MacAlister D, Editors. Hospital and healthcare security. Philadelphia, PA: Elsevier Science; 2015.
18. Kruger HA, Steyn T, Drevin L, Medlin BD. How secure are passwords that will be used by future health care workers? In redefining an agenda for Information Security. Proceedings of the 7th Annual Conference Security; 2008 June 2-3; Las Vegas, NV.
19. Cruz-Correia R, Boldt I, Lapao L, Santos-Pereira C, Rodrigues PP, Ferreira AM, et al. Analysis of the quality of hospital information systems Audit Trails. BMC Med Inform Decis Mak 2013; 13: 84.
20. Mahmood AK. Information security management of healthcare system [MSc Thesis]. Karlskrona, Sweden: Blekinge Institute of Technology; 2010.

Evaluation of Hospital Information Systems Security

Zahra Meidani[1], Mohammad Amin Assari[2], Seyed Ghoalmabbas Mosavi[3], Ali Ataei-Andezag[4]

Original Article

Abstract

Introduction: System security includes a set of security protections related to software, hardware, personnel and enterprise policies that protect Information Systems (IS) against internal and external threats. The present study aimed to define a comprehensive security model and then, assess hospital information systems (HIS) security in three areas of administrative, physical and technical safeguards.

Methods: This was a qualitative-descriptive study. The study population included 4 public educational hospitals from different regions of the country, each with a different HIS. The data collection tool was a checklist of 134 questions. In order to design a checklist, first, the security criteria were identified from the security standards. Then, HIS security requirements were determined in three areas of administrative, physical and technical safeguards through modified Delphi method. The answers to the questions of the checklist were defined as Yes "1" or No "0". HIS security level was identified in a five-level scale ranging from very low (0%) to very high (100%). Data were analyzed by descriptive statistics such as frequency and percentage.

Results: Administrative safeguards of HIS in studied hospitals with 31.8 % and physical safeguards with 25% had a low level of security. Moreover, technical safeguards of HIS in hospitals were observed to be a medium level of security with 42.6%.

Conclusion: The findings of this study expose HIS security weaknesses thus providing a good basis for managers of health information management and information technology departments in hospitals to implement appropriate corrective actions in policy formulation, user training, access control and risk management, and other dimensions of managerial and physical standards.

Keywords: Security; Hospital Information Systems; Administrative Security

Received: 22 May, 2017 Accepted: 08 Nov., 2017

Citation: Meidani Z, Assari MA, Mosavi SG, Ataei-Andezag A. **Evaluation of Hospital Information Systems Security.** Health Inf Manage 2017; 14(5): 187-93

Article resulted from research project No. 93103 funded by Kashan University of Medical Sciences.

1- Associate Professor, Health Information Management, Health Information Management Research Center AND Department of Health Information Management and Technology, School of Paramedicine, Kashan University of Medical Sciences, Kashan, Iran
2- Lecturer, Computer Engineering, Department of Computer Engineering and Information Technology, Payame Noor University, Tehran, Iran
3- Lecturer, Statistics and Epidemiology, Department of Statistics, School of Health, Kashan University of Medical Sciences, Kashan, Iran
4 -MSc, Health Information Technology, Department of Health Information Management and Technology, School of Paramedicine, Kashan University of Medical Sciences, Kashan, Iran (Corresponding Author) Email: ali.ataie_meshgini@yahoo.com