وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی*

اسماعیل مهرآیین[1]، هاله آیت اللهی[2]، مریم احمدی[3]

مقاله پژوهشی

چکیده

مقدمه: امروزه، با ظهور پرونده‌ی الکترونیکی بیمار، نیاز به تبادل اطلاعات افزایش یافته و در نتیجه امنیت و محرمانگی در سیستم‌های اطلاعاتی باید بیش‌تر مورد توجه قرار گیرد. در پژوهش حاضر، وضعیت امنیت اطلاعات از سه بعد مدیریتی، فنی و فیزیکی در سیستم‌های اطلاعات بیمارستانی بیمارستان‌های وابسته به دانشگاه‌های علوم پزشکی تهران و شهید بهشتی مورد شناسایی قرار گرفت.

روش بررسی: این پژوهش از نوع کاربردی بود که به روش تحلیلی در سال ۱۳۹۰ خورشیدی انجام شد. جامعه‌ی پژوهش، مسؤولان واحد فن‌آوری اطلاعات در بیمارستان‌های وابسته به دانشگاه‌های علوم پزشکی تهران و شهید بهشتی (۳۶ نفر) و نمایندگان شرکت‌های نرم‌افزاری (شش نفر) بودند. داده‌های پژوهش با استفاده از پرسش‌نامه گردآوری گردید و روایی پرسش‌نامه از طریق روایی صوری و محتوا و پایایی آن نیز با استفاده از آزمون همبستگی درونی (۰/۷۵=) تعیین شد. از آمار توصیفی و تحلیلی نظیر t-test برای تحلیل داده‌ها استفاده گردید.

یافته‌ها: براساس یافته‌های پژوهش، از لحاظ آماری تفاوت معناداری در وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد مدیریتی (Pvalue=۰/۸۴۳)، فنی (Pvalue=۰/۹۰۲) و فیزیکی (Pvalue=۰/۵۹۵) در مراکز آموزشی درمانی و غیرآموزشی وجود نداشت. اما از بعد فنی بین دیدگاه مسؤولان واحد کامپیوتر بیمارستان‌های مورد مطالعه و نمایندگان شرکت‌های نرم‌افزاری اختلاف معناداری وجود داشت (Pvalue=۰/۰۱).

نتیجه‌گیری: در این مطالعه وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی در سطح قابل قبولی ارزیابی گردید. با این حال برنامه‌ریزی جهت تدوین و اجرای جدیدترین سیاست‌ها و دستورالعمل‌های امنیتی در هر سه بعد مدیریتی، فنی و فیزیکی مطابق با نیازهای کاربران و پیشرفت‌های فن‌آوری ضروری به نظر می‌رسد.

واژه‌های کلیدی: امنیت داده‌ها؛ سیستم‌های اطلاعات بیمارستانی؛ فن‌آوری اطلاعات سلامت

دریافت مقاله: ۹۱/۶/۱۲ اصلاح نهایی: ۹۲/۲/۲۷

پذیرش مقاله: ۹۲/۶/۹

ارجاع: مهرآیین اسماعیل، آیت اللهی هاله، احمدی مریم. **وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی.** مدیریت اطلاعات سلامت ۱۳۹۲؛ ۱۰(۶): ۷۸۸-۷۷۹.

مقدمه

سازمان‌های مراقبت بهداشتی در سراسر دنیا تلاش می‌کنند تا برای رقابت با سازمان‌های دیگر و کسب نمره‌ی قابل قبول در ممیزی‌ها، رضایت بیماران را کسب کنند. در سال‌های اخیر این سازمان‌ها برای ارایه‌ی خدمات به مشتریان خود استفاده از پیشرفته‌ترین دستاوردهای علوم مختلف را آغاز کرده‌اند. سیستم‌های اطلاعات کامپیوتری یکی از این دستاوردها است که در سال‌های اخیر استفاده از این سیستم‌ها در سازمان‌های مراقبتی افزایش یافته است. از آنجا که اطلاعات در سیستم‌های کامپیوتری با حجم بالا ذخیره می‌شوند و با سرعت بالایی نیز قابل انتقال هستند، باید در تمام مراحل ورود داده، ذخیره‌سازی، استفاده و انتقال داده بحث امنیت اطلاعات مورد توجه قرار گیرد (۲، ۱).

* این مقاله حاصل پایان‌نامه‌ی کارشناسی‌ارشد در دانشگاه علوم پزشکی تهران می‌باشد.

۱- مربی، فن‌آوری اطلاعات سلامت، دانشکده‌ی بهداشت، دانشگاه علوم پزشکی زابل، زابل، ایران

۲- استادیار، انفورماتیک پزشکی، دانشکده‌ی مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران (نویسنده‌ی مسؤول)

Email: ayatollahi.h@iums.ac.ir

۳- دانشیار، مدیریت اطلاعات سلامت، دانشکده‌ی مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران

باید توجه داشت که امروزه به دلایل مختلف از جمله افزایش استفاده از سیستم‌های کامپیوتری، افزایش نیازهای تحقیقاتی و توجه ویژه به روش‌های پرداخت هزینه‌ی مراقبت‌ها، تعداد و انواع درخواست‌های مربوط به استفاده از اطلاعات سلامت افزایش یافته و این بدان معناست که مسؤولیت حفظ امنیت و محرمانگی اطلاعات سلامت خصوصاً در سیستم‌های کامپیوتری روز به روز پیچیده‌تر و دشوارتر می‌گردد (۳). در واقع، مسایل مربوط به امنیت و محرمانگی اطلاعات نگرانی‌هایی را برای مدیران مراکز مراقبتی و مدیران فن‌آوری اطلاعات ایجاد کرده است. چرا که حفظ امنیت اطلاعات بیمار در سیستم‌های اطلاعات بیمارستانی از اهمیت خاصی برخوردار است (۴).

به‌طور کلی برنامه‌های حفاظت از امنیت اطلاعات در سیستم‌های کامپیوتری از سه بعد مدیریتی، فنی و فیزیکی باید مورد توجه قرار گیرند (۵). امنیت اطلاعات از بعد مدیریتی به حفاظت‌های مدیریتی مناسب و منطقی از اطلاعات در سیستم‌های اطلاعاتی اشاره دارد. از جمله راهکارهای مدیریتی می‌توان به تحلیل خطرات امنیتی مربوط به ثبت، جمع‌آوری، دریافت و انتقال اطلاعات الکترونیکی اشاره کرد. امنیت اطلاعات سلامت از بعد فنی عبارت است از حفاظت از اطلاعات الکترونیکی در مقابل خطراتی که با پیشرفت فن‌آوری ممکن است سازمان‌های مراقبت بهداشتی با آن روبرو شوند، مثل دسترسی کاربران غیر مجاز به اطلاعات الکترونیکی از طریق اینترنت (۶). امنیت اطلاعات الکترونیکی سلامت از بعد فیزیکی نیز به مجموعه اقداماتی که برای حفظ و نگهداری اطلاعات سلامت بیماران در محیط امن و مطمئن صورت می‌گیرد اشاره دارد و در برگیرنده‌ی حفاظت فیزیکی از تجهیزات و سخت‌افزارهای سیستم‌های اطلاعات بیمارستانی می‌باشد (۱).

در زمینه‌ی حفاظت از امنیت اطلاعات در سیستم‌های کامپیوتری، استانداردهایی نظیر استانداردهای ایزو ۲۷۰۰۰، ۲۷۰۰۱ و ۲۷۰۰۲ معرفی شده‌اند (۷). اما در این میان معیارهای ارایه شده توسط انجمن سیستم‌های مدیریت و اطلاعات مراقبت سلامت (HIMSS: Healthcare Information and Management Systems Society) و استانداردهای قانون قابلیت انتقال و پاسخ‌گویی بیمه‌ی سلامت HIPAA (Health Insurance Portability and Accountability Act) به‌صورت تخصصی امنیت سیستم‌های اطلاعات بیمارستانی و امنیت اطلاعات بهداشتی را مورد توجه قرار داده‌اند. معیارهای ارایه شده توسط انجمن سیستم‌های مدیریت و اطلاعات مراقبت سلامت جهت بررسی امنیت اطلاعات در نرم‌افزارهای بخش بهداشت و درمان کاربرد داشته و استاندارد قانون قابلیت انتقال و پاسخ‌گویی بیمه‌ی سلامت در برگیرنده‌ی برنامه‌های حفاظت از امنیت اطلاعات سلامت از جنبه‌های مدیریتی، فنی و فیزیکی می‌باشد و می‌توان از آن به‌عنوان ابزاری جهت بررسی وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی استفاده کرد (۸، ۶).

از جمله پژوهش‌هایی که در زمینه امنیت اطلاعات در سیستم‌های اطلاعات سلامت انجام گرفته می‌توان به پژوهش Juanita و همکاران در سال ۲۰۰۹ میلادی اشاره کرد. یافته‌های این پژوهش حاکی از آن بود که عوامل مختلفی مثل عدم آموزش کارکنان، دستورالعمل‌های مبهم در مورد امنیت اطلاعات، چالش‌های بهره‌وری، کاربرد نامناسب اطلاعات و زیرساخت‌های امنیتی منسوخ شده، می‌توانند امنیت و محرمانگی اطلاعات در سیستم‌های کامپیوتری را در معرض خطر قرار دهند (۹). در پژوهشی دیگر که توسط Ganthan و همکاران در سال ۲۰۱۰ میلادی انجام شد، نتایج نشان داد که مهم‌ترین تهدید برای امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی، قطع برق توسط کارکنان و یا سایر عوامل فنی بود (۱۰). Kemp نیز در پژوهشی که در بیمارستان‌های وابسته به دانشگاه لندن انجام گرفت، ذکر کرده است که مدیریت امنیت اطلاعات در تعداد اندکی از بیمارستان‌ها و مراکز مراقبتی به‌طور صحیح اعمال می‌شد که این امر، چالشی در حوزه‌ی مدیریت اطلاعات محسوب می‌شود و موسسات باید برنامه‌ریزی‌های خود را در جهت رفع این مشکل سوق دهند (۱۱).

در ایران پژوهش‌های محدودی در خصوص امنیت اطلاعات خصوصاً در سیستم‌های کامپیوتری بخش بهداشت و درمان صورت گرفته و اکثر آن‌ها به‌صورت مطالعات تطبیقی بوده که وضعیت امنیت اطلاعات را در کشورهای مختلف مقایسه کرده‌اند

(۱۳-۱۲). به‌طور مثال، در مطالعه‌ای توصیفی- تطبیقی که در سال ۱۳۸۴ خورشیدی توسط بهنام انجام گرفت، مشخص شد که در کشورهای مورد مطالعه (آمریکا، کانادا، انگلستان و استرالیا)، حفظ امنیت و محرمانگی اطلاعات سلامت مواردی مانند نظارت بر صحت، کامل بودن اطلاعات و اجرای برنامه‌های آموزشی جهت آشنایی پرسنل با موضوعات مربوط به امنیت اطلاعات را شامل می‌شد (۱۳). اگرچه مطالعاتی نیز در خصوص طراحی الگوی مکانیسم محرمانگی و ایمنی اطلاعات پرونده‌ی الکترونیک سلامت برای ایران صورت گرفته (۱۲)، اما دستورالعمل‌ها و استانداردهای مدون برای حفظ امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی وجود ندارد و مسایل مربوط به امنیت اطلاعات سلامت در این سیستم‌ها کم‌تر مورد توجه قرار گرفته‌اند. از سوی دیگر، به نظر می‌رسد که در چند سال اخیر مراکز و موسسات درمانی کشور، بیش‌تر به فکر نصب و راه‌اندازی سیستم‌های اطلاعات بیمارستانی بودند و کم‌تر به جنبه‌های امنیتی آن‌ها پرداخته‌اند و مشخص نیست که شرکت‌های ارایه دهنده‌ی سیستم‌های اطلاعات بیمارستانی چه معیارهایی را برای حفظ امنیت اطلاعات در این سیستم‌ها در نظر می‌گیرند (۱۴). با توجه به اهمیت امنیت اطلاعات سلامت در بیمارستان‌ها و مؤسسات مراقبت بهداشتی و جایگزینی سیستم‌های اطلاعات بیمارستانی به‌جای سیستم‌های دستی در کشورمان، ضرورت بررسی مسایل مربوط به امنیت این سیستم‌ها، بیش از پیش احساس می‌شود. لذا پژوهش حاضر به شناسایی وضعیت امنیت اطلاعات از بعد مدیریتی، فنی و فیزیکی در سیستم‌های اطلاعات بیمارستانی بیمارستان‌های وابسته به دانشگاه‌های علوم پزشکی تهران و شهید بهشتی پرداخته است.

روش بررسی

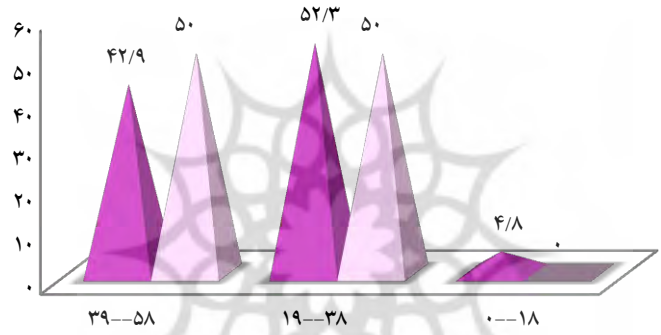
این پژوهش از نوع کاربردی بود که به روش تحلیلی در سال ۱۳۹۰ خورشیدی انجام شد. جامعه‌ی پژوهش در برگیرنده‌ی دو گروه بود. گروه اول را مسؤولان واحد فن‌آوری اطلاعات بیمارستان‌های وابسته به دانشگاه‌های علوم پزشکی تهران و شهید بهشتی که به سیستم اطلاعات بیمارستانی مجهز بودند و گروه دوم را نمایندگان شرکت‌های ارایه دهنده‌ی سیستم اطلاعات بیمارستانی تشکیل می‌دادند. در این پژوهش با توجه به محدود بودن تعداد افراد جامعه‌ی پژوهش در گروه اول (۴۱ نفر مسؤول واحد کامپیوتر)، نمونه‌گیری انجام نشد. اما از آن‌جا که معرفی‌نامه‌ی پژوهشی تنها برای ۱۱ بیمارستان از ۱۶ بیمارستان وابسته به دانشگاه علوم پزشکی شهید بهشتی صادر گردید، تعداد افراد جامعه‌ی پژوهش در گروه اول به ۳۶ نفر کاهش یافت که از این تعداد فقط ۲۹ نفر مسؤول واحد کامپیوتر (۸۰/۵ درصد) به پرسش‌نامه‌ها پاسخ دادند. همچنین، نظر به اینکه تنوع سیستم‌های اطلاعات بیمارستانی محدود بود (شش سیستم)، از هر شرکت ارایه دهنده‌ی نرم‌افزار یک نفر به‌عنوان نماینده برای شرکت در مطالعه انتخاب شد و از گروه دوم نیز نمونه‌گیری به‌عمل نیامد. به‌منظور گردآوری داده‌ها پرسش‌نامه‌ای براساس معیارهای انجمن سیستم‌های مدیریت و اطلاعات مراقبت سلامت (HIMSS) (۸)، استانداردهای قانون قابلیت انتقال و پاسخ‌گویی بیمه‌ی سلامت (HIPAA) (۷) و بررسی سایر پژوهش‌ها و مقالات مرتبط (۱۷-۱۵، ۲) توسط پژوهشگر طراحی شد که دربرگیرنده‌ی چهار قسمت مشخصات فردی شرکت‌کنندگان در پژوهش، سوالات مربوط به امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد مدیریتی، فنی و فیزیکی بود. برای شناسایی نقاط قوت و ضعف سیاست‌های امنیتی موجود و راهکارهای ارتقای امنیت، چهار سوال باز برای هر قسمت در نظر گرفته شد. روایی محتوا و روایی صوری پرسش‌نامه توسط چهار نفر از اساتید و صاحب نظران مورد تأیید قرار گرفت. سپس پرسش‌نامه بین افراد شرکت‌کننده در پژوهش توزیع شد. پایایی پرسش‌نامه با استفاده از آزمون همبستگی درونی (۰/۷۵=) تعیین شد. جهت تعیین دیدگاه نمایندگان شرکت‌های ارایه دهنده‌ی سیستم‌ها، تنها پرسش‌نامه‌ی مرتبط با بعد فنی در اختیار آنان قرار گرفت. به‌منظور تعیین دیدگاه افراد گزینه‌های مربوط به هر سوال به ترتیب امتیازدهی شدند (بلی=۲، خیر=۱ و اطلاعی ندارم=۰) و پس از محاسبه‌ی حداکثر و حداقل امتیاز برای هر قسمت از پرسش‌نامه، حد فاصل به دست آمده به سه گروه امتیازی تقسیم گردید. در این پژوهش از نرم‌افزار SPSS نسخه‌ی ۱۸ و آمار توصیفی و تحلیلی جهت تحلیل داده‌ها استفاده گردید. برای مقایسه‌ی وضعیت امنیت اطلاعات در

سیستم‌های اطلاعات بیمارستانی در مراکز آموزشی درمانی و مراکز غیر آموزشی و نیز مقایسه‌ی دیدگاه مسؤولان واحد فن‌آوری اطلاعات بیمارستان‌های مورد مطالعه و دیدگاه نمایندگان شرکت‌های ارایه دهنده‌ی سیستم‌ها در خصوص وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد فنی، میانگین امتیازات برای هر گروه محاسبه و سپس از آزمون t-test استفاده شد.

یافته‌ها

بیش‌تر افرادی که در این پژوهش شرکت کرده بودند (۵۱/۴ درصد) در گروه سنی ۳۰–۲۵ سال قرار داشتند و دارای مدرک کارشناسی در رشته‌ی کامپیوتر (۸۹/۷ درصد) بودند. اکثر این افراد (۷۷/۱ درصد) دارای سابقه‌ی کار ۱۰–۱ سال بودند.

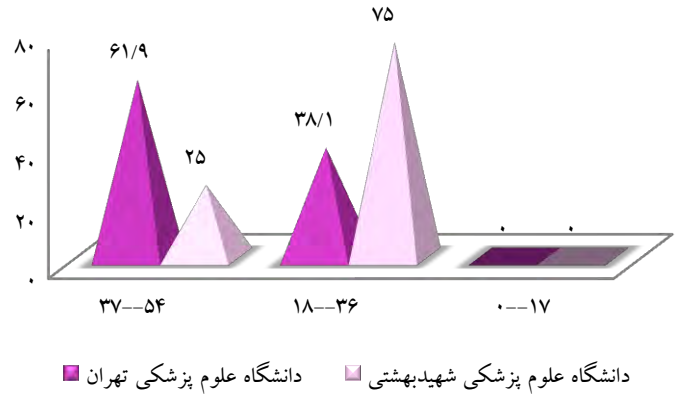
بعد مدیریتی شامل دو حوزه‌ی سیاست‌گذاری و آموزش (۲۹ سوال) و دارای حداقل امتیاز صفر و حداکثر امتیاز ۵۸ بود. براساس یافته‌های این پژوهش اکثر بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران (۵۲/۳ درصد) و شهید بهشتی (۵۰ درصد) از نظر وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد مدیریتی در رده‌ی امتیازی متوسط (۳۸–۱۹) قرار داشتند (نمودار ۱).



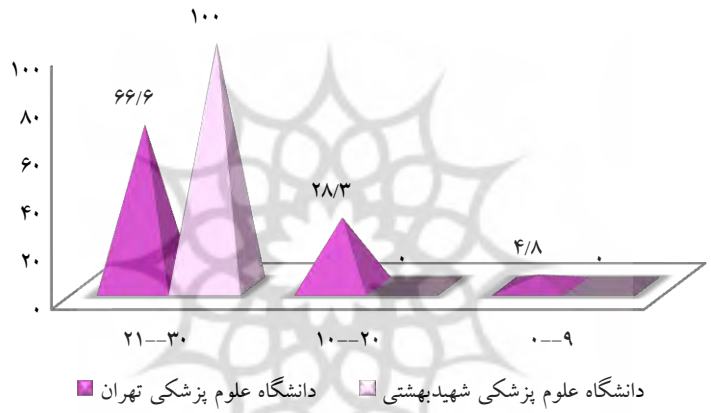
نمودار ۱: وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد مدیریتی

بعد فنی شامل سه حوزه‌ی نرم‌افزاری، کلمه‌ی عبور و دسترسی (۲۷ سوال) و دارای حداقل امتیاز صفر و حداکثر امتیاز ۵۴ بود. براساس یافته‌های این پژوهش اکثر بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران (۶۱/۹ درصد) در رده‌ی امتیازی خوب (۵۴–۳۷) و اکثر بیمارستان‌های وابسته به دانشگاه علوم پزشکی شهید بهشتی (۷۵ درصد) از نظر وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد فنی در رده‌ی امتیازی متوسط (۳۶–۱۸) قرار داشتند (نمودار ۲).

بعد فیزیکی شامل دو حوزه‌ی سیاست‌گذاری و حفاظتی (۱۵ سوال) و دارای حداقل امتیاز صفر و حداکثر امتیاز ۳۰ بود. براساس یافته‌های این پژوهش اکثر بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران (۶۶/۶ درصد) و کلیه‌ی بیمارستان‌های وابسته به دانشگاه علوم پزشکی شهید بهشتی (۱۰۰ درصد) از نظر وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد فیزیکی در رده‌ی امتیازی خوب (۳۰–۲۱) قرار داشتند (نمودار ۳).



نمودار ۲: وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد فنی



نمودار ۳: وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد فیزیکی

براساس یافته‌های این پژوهش بیش‌تر مسؤولان واحد کامپیوتر بیمارستان‌های مورد مطالعه (۵۱/۷ درصد) معتقد بودند که سیستم‌های اطلاعات بیمارستانی از بعد فنی در رده‌ی امتیازی خوب (۵۴-۳۷) قرار دارند، در حالی‌که از نظر تمام نمایندگان شرکت‌های ارایه دهنده‌ی نرم‌افزار (۱۰۰ درصد) این سیستم‌ها در رده‌ی امتیازی متوسط (۳۶-۱۸) قرار داشتند (جدول ۱). از نظر آماری نیز در خصوص وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد فنی بین دیدگاه مسؤولان واحد کامپیوتر بیمارستان‌های مورد مطالعه و نمایندگان شرکت‌های ارایه‌دهنده‌ی سیستم‌ها اختلاف معناداری وجود داشت (Pvalue=۰/۰۱). بدین معنا که مسؤولان واحد کامپیوتر بیمارستان‌های مورد مطالعه سیستم‌ها را از بعد فنی در رده‌ی امتیازی بالاتری ارزیابی کرده بودند، در حالی‌که نمایندگان شرکت‌های ارایه‌دهنده‌ی سیستم‌ها رده‌ی امتیازی پایین‌تری را برای سیستم‌ها در نظر گرفتند. همچنین تفاوت معناداری در وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد مدیریتی، فنی و فیزیکی در مراکز آموزشی درمانی و غیر آموزشی مشاهده نشد.

جدول ۱: مقایسه‌ی دیدگاه مسؤولان واحد کامپیوتر بیمارستان‌های مورد مطالعه با دیدگاه نمایندگان شرکت‌های ارایه‌دهنده‌ی سیستم‌ها در خصوص وضعیت امنیت اطلاعات سلامت در سیستم‌های اطلاعات بیمارستانی از بعد فنی

وضعیت امنیت اطلاعات از بعد فنی	رده امتیازی ۳۷-۵۴		رده امتیازی ۱۸-۳۶		رده امتیازی ۰-۱۷		میانگین± انحراف معیار
بیمارستان‌ها	تعداد	درصد	تعداد	درصد	تعداد	درصد	
مسؤولان واحد کامپیوتر بیمارستان‌ها (N=۲۹)	۱۵	۵۱/۷	۱۴	۴۸/۳	۰	۰	۳±۱۸/۸
نمایندگان شرکت‌ها (N=۶)	۰	۰	۶	۱۰۰	۰	۰	۲/۱±۱۵/۷

بحث

پیشرفت‌های اخیر در فن‌آوری اطلاعات و ارتباطات باعث شده تا بسیاری از بخش‌های تجاری و غیر تجاری، موسسات آموزشی و تحقیقاتی، ادارات و سازمان‌ها در سراسر جهان به استفاده از دستاوردهای فن‌آوری اطلاعات و ارتباطات روی آورند (۱۸). یکی از این دستاوردها، سیستم‌های اطلاعات کامپیوتری می‌باشد که استفاده از آن‌ها در موسسات مراقبت بهداشتی به سرعت در حال افزایش است (۱۹). سیستم‌های اطلاعات کامپیوتری در بیمارستان‌ها با عنوان سیستم‌های اطلاعات بیمارستانی جایگاه خاصی پیدا کرده‌اند و کارکنان بخش سلامت به‌منظور انجام وظایف روزمره‌ی خود از این سیستم‌ها استفاده می‌کنند. بدین ترتیب که تمام اطلاعات بالینی، مالی و هویتی بیماران در این سیستم‌ها ثبت و نگه‌داری می‌شوند. همچنین با استفاده از این سیستم‌ها، تبادل داده‌ها نیز آسان‌تر می‌گردد (۲۰).

از آن‌جاکه اطلاعات در اشکال گوناگون، یکی از مهم‌ترین دارایی‌های هر سازمانی به حساب می‌آید، بحث امنیت اطلاعات در ابعاد مختلف از جایگاه ویژه‌ای برخوردار است. فقدان امنیت اطلاعات نه تنها ممکن است تهدیدی برای یکپارچگی اطلاعات در سازمان‌های مراقبتی باشد، بلکه ممکن است موجودیت این سازمان‌ها را نیز به خطر اندازد. لذا سازمان‌های مراقبتی باید به موضوع امنیت اطلاعات در سطوح مختلف توجه داشته و با برنامه‌ریزی و استفاده از دستورالعمل‌های موجود در این زمینه از بروز مشکلات امنیتی پیشگیری نمایند (۲۱).

یافته‌های پژوهش حاضر نشان داد که از دیدگاه مسؤولان واحد کامپیوتر بیش‌تر بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران و شهید بهشتی، وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد مدیریتی در رده‌ی امتیازی بالایی قرار داشت. در این زمینه، نتایج پژوهش Park و همکاران نشان داد که از بین سطوح امنیت اطلاعات (مدیریتی، فنی و فیزیکی) آسیب‌پذیرترین سطح، سطح مدیریتی است و سطح امنیت اطلاعات در سیستم‌های مورد مطالعه در سطح متوسط ارزیابی شد (۲۲). سایر مطالعات نیز نشان‌دهنده‌ی آن است که سطوح دسترسی، نظارت بر صحت و کامل بودن اطلاعات و اجرای برنامه‌های آموزشی جهت آشنایی کارکنان با موضوعات مربوط به امنیت اطلاعات که جزو زیرمجموعه‌های بعد مدیریتی امنیت اطلاعات محسوب می‌شوند، در سایر کشورها از اهمیت خاصی برخوردار بوده و برنامه‌ریزی برای ارتقای این موارد توصیه شده است (۹). لذا وضعیت خوب امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی مراکز مورد مطالعه در بعد مدیریتی حاکی از آن است که برخلاف تصورات رایج، تمهیدات لازم جهت حفاظت از امنیت اطلاعات اندیشیده شده است و بعد مدیریتی امنیت اطلاعات مشتمل بر حوزه‌های سیاست‌گذاری و آموزشی چه در بیمارستان‌های آموزشی و چه غیر آموزشی مورد توجه قرار گرفته‌اند.

یافته‌های پژوهش نشان داد که از دیدگاه مسؤولان واحد کامپیوتر، بیش‌تر بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران از نظر وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد فنی در رده‌ی امتیازی بالاتری نسبت به بیمارستان‌های وابسته به دانشگاه علوم پزشکی شهید بهشتی قرار داشتند. در این خصوص یافته‌های مطالعه‌ی Susilo و همکاران نشان‌گر آن است که نواقص موجود در زمینه‌ی امنیت اطلاعات در تحقیقات بهداشتی از بعد فنی، در نتیجه‌ی عدم

رمزگذاری داده‌ها و پایگاه‌های داده‌ای و فقدان یک روش معتبر و امن برای دسترسی به داده‌های بالینی است (۲۳). به‌طور مشابه، Collmann و همکاران در پژوهش خود بیان کردند که برای حفاظت از اطلاعات حساس، سازمان‌های مراقبت بهداشتی باید علاوه بر ایجاد سطح امنیتی مناسب، زمینه‌های سازمانی ایمنی از قبیل استفاده از کلمات عبور، برنامه‌های ضد ویروس و نرم‌افزارهای پیشرفته جهت مقابله با انواع تهدیدهای امنیتی برای سیستم‌های اطلاعات بهداشتی خود فراهم نمایند (۲۴). در مطالعه‌ی دیگری نظرات کاربران سیستم‌های اطلاعات بیمارستانی در مورد امنیت اطلاعات و خدمات امنیتی در این سیستم‌ها حاکی از آن بود که فرایندهای فنی امنیتی در نظر گرفته شده برای حفاظت از داده‌های پزشکی ناکافی بوده است (۱۰). از آن‌جاکه سیستم‌های اطلاعات بیمارستانی از شرکت‌های نرم‌افزاری متفاوتی خریداری می‌شوند، ضروری است تا علل ضعف امنیتی سیستم‌ها از بعد فنی در هر مرکز به دقت مورد بررسی قرار گیرد و از شرکت‌های طرف قرارداد خواسته شود تا جهت رفع نقایص موجود اقدامات لازم را انجام دهند.

براساس یافته‌های پژوهش اگر چه وضعیت امنیت اطلاعات از بعد فنی و در بیمارستان‌های مورد مطالعه در سطوح مختلفی ارزیابی شد، اما در کل مسؤولان واحد کامپیوتر بیمارستان‌ها در مقایسه با نمایندگان شرکت‌های نرم‌افزاری، امنیت فنی سیستم‌ها را در سطح بهتری ارزیابی کردند. علت این امر را می‌توان چنین بیان کرد که ممکن است نمایندگان شرکت‌ها به علت مشارکت مستقیم در طراحی سیستم‌ها بیش از مسؤولان واحد کامپیوتر از مسایل فنی مربوط به سیستم‌ها مطلع بوده‌اند و دیدگاه آن‌ها نسبت به امنیت اطلاعات از بعد فنی واقع بینانه‌تر باشد.

از نظر وضعیت امنیت اطلاعات از بعد فیزیکی نیز یافته‌ها نشانگر آن بود که بیش‌تر بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران و کلیه‌ی بیمارستان‌های وابسته به دانشگاه علوم پزشکی شهید بهشتی در رده‌ی امتیازی بالایی قرار داشتند. در این رابطه، نتایج مطالعه‌ی Ganthan نشان می‌دهد که بعد فیزیکی امنیت اطلاعات در سازمان‌های مراقبتی نقش به‌سزایی در ارتقای سطح امنیتی اطلاعات دارد، تا آن‌جاکه یکی از مهم‌ترین تهدیدها برای امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی عبارت است از قطع برق به دلیل نارسایی یا خطاهای انسانی یا سایر عوامل تکنولوژیکی (۱۰). لذا می‌توان گفت که همانند بعد مدیریتی، بعد فیزیکی امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی نیز در مراکز مورد مطالعه مورد توجه قرار گرفته است و از تجربیات به‌دست آمده در این مراکز می‌توان جهت تدوین دستورالعمل‌ها و آیین‌نامه‌های اجرایی در سایر مراکز مشابه سود برد.

نتیجه‌گیری

به‌طور کلی، یافته‌های پژوهش نشان‌گر آن بود که وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی بیمارستان‌های وابسته به دانشگاه‌های علوم پزشکی تهران و شهید بهشتی از دیدگاه مسؤولان واحد کامپیوتر این بیمارستان‌ها در سطح قابل قبولی بود. این در حالی است که امنیت اطلاعات از بعد مدیریتی و فیزیکی در بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران نسبت به بیمارستان‌های وابسته به دانشگاه علوم پزشکی شهید بهشتی، امتیاز پایین‌تری را به خود اختصاص داد. در مقابل، بیش‌تر بیمارستان‌های وابسته به دانشگاه علوم پزشکی شهید بهشتی از نظر وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی از بعد فنی امتیاز کم‌تری نسبت به بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران کسب کرده بودند. بنابراین باید توجه داشت که وضعیت موجود دارای نقاط ضعفی نیز می‌باشد و برنامه‌ریزی جهت تدوین و اجرای جدیدترین سیاست‌ها و دستورالعمل‌های امنیتی در هر سه بعد مدیریتی، فنی و فیزیکی مطابق با نیازهای کاربران و پیشرفت‌های فن‌آوری ضروری به نظر می‌رسد.

پیشنهادها

برای ارتقای وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی و در کلیه‌ی ابعاد، تدوین دستورالعملی کشوری ضروری به نظر می‌رسد. با این حال امنیت سیستم‌ها را می‌توان با توجه ابعاد مختلف آن در هر مرکز به‌طور جداگانه نیز مورد توجه قرار داد. به‌طور مثال جهت تأمین امنیت از بعد فنی راهکارهایی نظیر استفاده از نرم‌افزارهای جدیدتر برای ثبت

تغییرات مهم در سیستم، محدود کردن سطوح دسترسی براساس نقش‌ها و وظایف کاربران، تغییر رمزهای عبور کاربران به‌صورت دوره‌ای و انجام تست نفوذ دوره‌ای برای اطمینان از سطح امنیت نرم‌افزار پیشنهاد می‌گردد. استفاده از اتاق سرور استاندارد و مجهز به سیستم هشدار حریق، مجهز بودن سیستم‌ها به برق اضطراری برای جلوگیری از آسیب‌های فیزیکی و حمایت بیش‌تر مدیران در زمینه‌ی حفظ امنیت فیزیکی از دیگر مواردی است که بر امنیت سیستم‌ها و اطلاعات خواهد افزود.

تشکر و قدردانی

این مقاله حاصل پایان‌نامه تحت عنوان «امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی بیمارستان‌های وابسته به دانشگاه‌های علوم پزشکی تهران و شهید بهشتی» در مقطع کارشناسی ارشد رشته‌ی مدارک پزشکی در سال ۱۳۹۰ خورشیدی می‌باشد که با حمایت دانشگاه علوم پزشکی و خدمات بهداشتی درمانی تهران اجرا شده است.

References

1. Cavalli E, Mattasoglio A, Pinciroli F, Spaggiari P. Information Security Concepts and Practices: The Case of a Provincial Multi-Specialty Hospital. Int J Med Inform 2004; 73(3): 297-303.
2. Ray A, Newell S. Exploring Information Security Risks in Healthcare Systems. In: Rodrigues J. editor. Health information systems: Concepts, methodologies, tools and applications. USA: IGI Global; 2010:1716-18.
3. Huffman EK, Cofer J. Health Information Management. Trans. Langarizadeh M. Tehran: Dibagaran; 2003: 20-22. [Book in Persian]
4. Fernando J. Factors That Have Contributed To a Lack of Integration in Health Information System Security. J Inform Techn Healthcare 2004; 2(5): 313-28.
5. Board of Governors of the Federal Reserve System. Interagency Guidelines Establishing Information Security Standards [Online]. 2009 [Cited 2011 Mar 11]; Available from: URL: http://www.federalreserve.gov/bankinforeg /interagencyguidelines.htm.
6. Department of Health and Human Services. Health Information Privacy [Online]. 2011 [Cited 2011 Apr 6]; Available from: URL: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule.
7. International Organization for Standardization. The ISO 27000 Directory. 2009 [Cited 2011 March 26]. Available from: URL: http://www.27000.org. 2011.
8. Healthcare Information and Management Systems Society (HIMSS). Information Systems Security. 2011 [Cited 2011 Apr 14]. Available from: URL: http://www.himss.org/content/files/applicationsecurityv2.3.pdf.
9. Fernando JI, Dawson LL. The Health Information System Security Threat Lifecycle: An Informatics Theory. Int J Med Inform 2009; 78(12): 815-26.
10. Samy GN, Ahmad R, Ismail Z. Security threats categories in healthcare information systems. Health Informatics J 2010; 16(3): 201-9.
11. Kemp L. Information Security Management: An Entangled Research Challenge. Inform Sec Tech Rept 2009; 14(4): 181-5.
12. Farzandipour M. Electronic Health Records Privacy and the Safety Mechanism Design Model for Iran [PhD Thesis in Persian]. Tehran, Iran: Iran University of Medical Sciences, Faculty of Health Management and Information Sciences; 2006.
13. Behnam S. Comparative Study of Levels of Access and Confidentiality of Medical Records in Selected Countries with Iran [MSc Dissertation in Persian]. Tehran, Iran: Iran University of Medical Sciences, Faculty of Health Management and Information Sciences; 2004.
14. Pourasghar F. The Role of Information Technology on Documentation and Security of Medical Data [PhD Thesis]. Sweden: Department of Learning, Information, Management and Ethics Karolinska Institute, Stockholm; 2009.
15. Lusignan S, Chanb T, Theadoma A, Dhoula N. The Roles of Policy and Professionalism in the Protection of Processed Clinical Data: A Literature Review. Int J Med Inform 2007; 76(4): 261-68.
16. Coleman J. Assessing Information Security Risk in Healthcare Organizations of Different Scale. Int Cong Ses 2004; 1268: 125-30.

17. Cazier J, Medlin B. How Secure Is Your Information System? An Investigation into Actual Healthcare Worker Password Practices. Perspect Health Inf Manage 2006; 3: 8.
18. Gritzalis D, Lambrinoudakis C. A Security Architecture for Interconnecting Health Information Systems. Int J Med Inform 2004; 73(3): 305-9.
19. Katsikas S. Health Care Management and Information Systems Security: Awareness, Training or Education? Int J Med Inform 2000; 60(2): 129-35.
20. Huang L, Chub H, Liena C, Hsiaoc C, Kao T. Privacy Preservation and Information Security Protection for Patients Portable Electronic Health Records. Comput Big Med 2009; 39(9): 743-50.
21. Ness RB. Influence of the HIPAA privacy rule on health research. J Am Med Assn 2007; 298(18): 2164-70.
22. Park W, 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.
23. Susilo S, Win K. Security and Access of Health Research Data. J Med Syst 2007; 31(2):103-7.
24. Collmann J, Cooper T. Breaching the Security of the Kaiser Permanent Internet Patient Portal: The Organizational Foundations of Information Security. J Am Med Inform Assoc 2007; 14(2): 239-43.

A Study of Information Security in Hospital Information Systems*

Esmaeil Mehraeen[1]; Haleh Ayatollahi[2]; Maryam Ahmadi[3]

Original Article

Abstract

Introduction: Nowadays, with the advent of electronic medical records (EMR), the need for information sharing has increased. As a result, more attention should be paid to the security and confidentiality of information systems. In this research, information security in hospital information systems was investigated considering three dimensions (administrative, technical and physical) in the hospitals affiliated to Tehran and Shahid Beheshti Universities of Medical Sciences.

Methods: This was an applied research study completed in 2012. The study population composed of information technology managers working in the hospitals affiliated to Tehran and Shahid Beheshti Universities of Medical Sciences, and the representatives of software companies. Data were collected using a questionnaire. To check the face and content validity of the questionnaire, experts views were investigated and the reliability of the questionnaire was confirmed using Cronbach s Coefficient Alpha (α= 0/75). Descriptive and inferential statistics, such as t-test were used to analyze data.

Results: The study results showed that most of the hospitals had addressed issues related to information security in hospital information systems, and all three dimensions had been taken into account. There was no significant difference between the level of information security in the teaching and the non-teaching hospitals. However, there was a significant difference between the views of the information technology managers and the perspectives of the software companies representatives about the technical dimension of information security.

Conclusion: Although the information security in hospital information systems was evaluated at the acceptable level, planning and implementing more effective security policies are necessary to overcome weaknesses in different dimensions of information security.

Keywords: Data Security; Hospital Information Systems; Health Information Technology

Received: 2 Sep, 2012 Accepted: 31 Aug, 2013

Citation: Mehraeen E, Ayatollahi H, Ahmadi M. **A Study of Information Security in Hospital Information Systems.** Health Inf Manage 2014; 10(6):788.

* This article is derived from MSc thesis.

1. Lecturer, Health Information Technology, Faculty of Public Health, University of Zabol, Zabol, Iran
2. Assistant Professor, Medical Informatics, Faculty of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran (Corresponding Author) Email: ayatollahi.h@iums.ac.ir
3- Associate Professor, Health Information Management, Faculty of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran