مجله اخلاق پزشکی

دوره سیزدهم، شماره چهل‌وچهارم، ۱۳۹۸

doi: https://doi.org/10.22037/mej.v13i44.19524

Journal Homepage: http://journals.sbmu.ac.ir/me

مقاله پژوهشی

دسترسی آزاد

مدیریت امنیت اطلاعات: تأثیر تعهد سازمانی و عواقب ادراک‌شده افشای اطلاعات محرمانه بر قصد نقض امنیت اطلاعات بیماران

زهرا کریمی[۱]، حمیدرضا پیکری[۲*]

۱. کارشناسی ارشد مدیریت دولتی، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران.

۲. استادیار گروه مدیریت، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران.

اطلاعات مقاله

تاریخ دریافت: ۹۶/۱۰/۰۲

تاریخ پذیرش: ۹۷/۱۱/۲۷

تاریخ انتشار: ۹۸/۰۶/۰۲

واژگان کلیدی:

سیاست امنیتی

قصد نقض امنیت اطلاعات

تعهد

* نویسنده مسؤول: حمیدرضا پیکری

آدرس پستی: ایران، اصفهان، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، گروه مدیریت.

تلفن: 2729 33500 98+

نمابر:

E-mail: omid726@yahoo.com

چکیده

زمینه و هدف: امنیت اطلاعات یک مسأله حیاتی در حوزه سلامت و درمان است. در بیشتر تحقیقاتی که در این زمینه صورت گرفته، عامل انسانی نادیده گرفته شده و یک نوع دید و رویکرد فنی وجود داشته است. مقاله حاضر با هدف تعیین رابطه ادراک پرسنل از عواقب افشای اطلاعات و تعهد کارکنان با قصد آن‌ها بر قصد نقض امنیت اطلاعات انجام گرفت.

مواد و روش‌ها: نمونه این پژوهش را ۱۸۱ نفر از پزشکان متخصص بیمارستان‌های آموزشی تخصصی شهر اصفهان تشکیل می‌دادند که به وسیله پرسشنامه بومی‌سازی‌شده با روش در دسترس نمونه‌گیری شدند. جهت سنجش عواقب ادراک‌شده افشای اطلاعات از پرسشنامه D'Arcy و همکاران با ۷ سؤال و دارای دو بعد درک از قطعیت و شدت مجازات‌ها و جهت سنجش تعهد سازمانی، پرسشنامه ۲۴ سؤالی Allen و Meyer با سه بعد تعهد عاطفی، هنجاری و مستمر استفاده شد. پس از تأیید روایی صوری، محتوایی و سازه پایایی به روش آلفای کرونباخ و پایایی مرکب، فرضیه‌ها با استفاده از روش حداقل مربعات جزئی و توسط نرم‌افزار SmartPLS آزموده شدند.

یافته‌ها: یافته‌های این تحقیق نشان داد که ادراک پزشکان متخصص از سیاست‌های سازمانی که نشانگر قطعیت و شدت مجازات افشای اطلاعات است، رابطه منفی معنادار با قصد نقض امنیت اطلاعات بیماران توسط آن‌ها دارد ($P<0.001$). همچنین نتایج نشان داد که ادراک پزشکان متخصص از تعهد که شامل تعهد عاطفی، هنجاری و مستمر بود، رابطه معنادار بر قصد نقض امنیت اطلاعات بیماران توسط آن‌ها ندارد.

ملاحظات اخلاقی: شرکت در جمع‌آوری داده‌ها داوطلبانه بود، رضایت شفاهی شرکت‌کنندگان کسب و به آنان نسبت به محرمانگی هویت آن‌ها اطمینان داده شد.

نتیجه‌گیری: سیاست‌های سازمانی از لحاظ قطعیت و شدت مجازات پزشکان نقض‌کننده امنیت اطلاعات باید در سطح بیمارستان‌ها و حتی در سطح وزارتخانه تشدید و با ابزار گوناگون به اطلاع دست‌اندرکاران حوزه درمان و از جمله پزشکان برسد.

۱. مقدمه

استفاده از قابلیت‌های فناوری اطلاعات درصنعت سلامت، به شکل کاربردهای مختلف سلامت الکترونیک، روز به روز گسترده‌تر می‌شود (۲-۱). از آنجا که امنیت و کنترل اطلاعات بهداشتی مربوط به بیمار یک جزء اساسی در تمام سیستم‌های اطلاعاتی مراقبت سلامت است (۵-۳)، در این ارتباط نگرانی زیادی در مورد حفظ حریم شخصی و تأمین امنیت اطلاعات به وجود آورده است، زیرا مدارک پزشکی بیمار شامل برخی از خصوصی‌ترین و محرمانه‌ترین اطلاعات بیمار بوده و با توجه با این‌که اطلاعات رایانه‌ای از مکان‌های متعددی قابل دسترس است به راحتی می‌تواند مورد سوءاستفاده قرار گیرد. نقص در این سیستم‌ها خطر افشای اطلاعات را به دنبال خواهد داشت (۷-۶). این در حالی است که در برنامه‌های امنیت سیستم‌های اطلاعاتی، عامل انسانی اغلب به عنوان یکی از اصلی‌ترین عوامل محسوب می‌شوند (۱۰-۸). در صورت ایجاد کلیه تمهیدات فنی و سیاست‌های امنیتی، عدم آگاهی و بی‌توجهی کاربران می‌تواند تمامی حفاظت‌های فنی را بی‌نتیجه سازد (۸). به همین دلیل دو عامل بازدارندگی و تعهد کارکنان به عنوان عوامل محتمل مؤثر در کاهش نقض امنیت اطلاعات پیشنهاد می‌شود (۱۲-۱۱).

بر اساس نظریه بازدارندگی، تدابیر فنی زمانی قدرت بازدارندگی دارد که با ارائه دانش از رفتارهای غیر قابل قبول و سپس ایجاد ترس و یا تمایل برای جلوگیری از پیامدهای منفی درک صحیحی ایجاد کند. بر اساس این نظریه، از آنجا که سیاست‌های امنیتی معادل با قوانین سازمانی است، انتظار می‌رود درک عواقب نقض قوانین سازمانی باعث کاهش رفتارهای افشای اطلاعات گردد، چراکه تدوین این تدابیر باعث افزایش بینش کارکنان از عواقب افشای اطلاعات می‌گردد. تئوری بازدارندگی بیان می‌کند که افراد زمانی که می‌خواهند خلافی انجام دهند، شدت و احتمال منفعت و زیان آن را می‌سنجند و بعد نسبت به آن اقدام می‌کنند. تئوری بازدارندگی شامل تحریم‌های رسمی مانند قوانین و سیاست‌های مجازاتی وضع‌شده از طرف سازمان‌ها و غیر رسمی مثل تأییدنشدن از طرف همکاران، احساس تقصیر و اضطراب از طرف دیگران می‌شود، لذا آگاهی پرسنل از وجود و شدت مجازات‌ها و نیت سوءاستفاده از اطلاعات محرمانه می‌تواند رفتارهای امنیتی او را افزایش دهد (۱۲). انطباق کارکنان با سیاست‌های امنیت اطلاعات به عنوان یکی از مشکلات اساسی سازمان‌ها در زمینه اصول امنیتی گزارش شده است (۱۳). تخمین زده می‌شود که بیش از نیمی از تمام موارد نقض سیستم‌های امنیتی اطلاعاتی به طور مستقیم یا غیر مستقیم توسط کارکنان نامناسب ایجاد می‌شود (۱۴). نقض سیاست‌های امنیتی توسط کارمند اغلب به علت سهل‌انگاری و جهل و یا به صورت عمدی و رفتارهای خلاف مقررات سازمان سر می‌زند (۱۵). بر اساس تئوری بازدارندگی، سیاست‌های سازمانی در خصوص عواقب افشای اطلاعات شامل ۲ بعد قطعیت مجازات و شدت مجازات می‌شود (۱۳-۱۲).

از طرف دیگر، تعهد می‌تواند عامل اصلی رازداری در بین افراد باشد (۱۱). افراد متعهدتر با ارزش‌ها و اهداف سازمان پایبندترند و فعالانه‌تر در سازمان نقش‌آفرینی خواهند کرد و کم‌تر به ترک سازمان و یافتن فرصت‌های شغلی جدید اقدام می‌کنند (۱۱). در واقع مفهوم تعهد سازمانی برنگرش مثبتی دلالت دارد که از احساس وفاداری کارکنان به سازمان حاصل می‌شود و با مشارکت افراد در تصمیمات سازمانی توجه به افراد سازمان و موفقیت و رفاه آنان تجلی می‌یابد. مطالعات انجام‌شده در این زمینه نشان می‌دهند که تعهد کارکنان به سازمان نتایج بسیار ارزشمندی برای سازمان در پی خواهد داشت (۱۶). صالحی‌فرد و خلج اسدی (۱۷) و Allen و Meyer (۱۸)، ابعاد تعهد سازمانی را شامل تعهد عاطفی، تعهد مستمر و تعهد هنجاری می‌دانند. در مطالعه‌ای نشان داده شده که کادر فنی متعهدتر دارای تمایل بیشتر برای حفظ اصول اخلاقی در محیط بیمارستان هستند (۱۹). با این حال بیشتر تحقیقات مرتبط با تعهد سازمانی به منظور کشف پیش‌بینی‌ها و بازده‌های تعهد سازمانی هدایت شده‌اند

(۲۰،۱۹). با توجه به این‌که تأثیر متغیرهای عواقب افشای اطلاعات و تعهد سازمانی بر افشای اطلاعات محرمانه به طور هم‌زمان در پژوهشی مورد بررسی قرار نگرفته، لذا پژوهش حاضر می‌تواند فتح بابی در این زمینه به شمار آید. از سویی دیگر با عنایت به نقش مهم و تعیین‌کننده امنیت اطلاعات در پرونده‌های سلامت بیماران در بیمارستان‌ها و نقش آن به عنوان یکی از مهم‌ترین ارکان درمانی، مطالعه متغیرهای فوق الذکر در خصوص عوامل انسانی (کارکنان) شایان توجه می باشد. بنابراین مقاله حاضر با هدف تعیین رابطه ادراک پرسنل از عواقب افشای اطلاعات و تعهد کارکنان با قصد آن‌ها بر قصد نقض امنیت اطلاعات انجام گرفت. جهت این امر، در این پژوهش فرضیه‌های زیر مورد بررسی قرار گرفتند:

ـ ادراک پرسنل از سیاست‌های سازمانی که نشانگر قطعیت و شدت مجازات افشای اطلاعات است، رابطه منفی معنادار با قصد نقض امنیت اطلاعات بیماران توسط آن‌ها دارد.

ـ ادراک پرسنل از تعهد عاطفی، هنجاری و مستمر رابطه منفی معنادار با قصد نقض امنیت اطلاعات بیماران توسط آن‌ها ندارد.

۲. ملاحظات اخلاقی

جهت رعایت ملاحظات اخلاقی، مراحل زیر انجام پذیرفت:

۱ـ اخذ معرفی‌نامه برای حضور در محیط پژوهش از دانشگاه محل تحصیل.

۲ـ اخذ اجازه از ریاست بیمارستان‌ها و مسؤولین بخش‌ها، جهت حضور پژوهشگر و انجام اقدامات لازم.

۳ـ معرفی خود به مشارکت‌کنندگان و توضیح مختصر در مورد هدف مطالعه، نحوه همکاری، فواید و معایب شرکت در مطالعه، هدف از تکمیل پرسشنامه.

۴ـ کسب رضایت‌نامه کتبی آگاهانه از شرکت‌کنندگان برای شرکت در مطالعه.

۵ـ کسب اجازه از شرکت‌کنندگان جهت تکمیل پرسشنامه.

۶ـ اطمینان‌دادن به مشارکت‌کنندگان در مورد حفظ حریم خصوصی و خلوت و محرمانه‌ماندن اطلاعات.

۷ـ اطمینان‌دادن به مشارکت‌کنندگان، جهت خودداری از شرکت در مطالعه در هر زمان در صورت تمایل آنان و حتی آزادبودن برای خروج از پژوهش در هر مرحله از پژوهش.

۸ـ جمع‌آوری داده‌ها از نظر زمان و مکان با توافق مشارکت کنندگان.

۹ـ اطمینان‌دادن به مشارکت‌کنندگان در جهت تجزیه و تحلیل داده‌ها به صورت کلی و رعایت اصول بی‌نامی در پیاده کردن، تحلیل و گزارش و نشر اطلاعات.

۳. مواد و روش‌ها

روش تحقیق در این پژوهش، توصیفی از نوع همبستگی است و در زمره مطالعات میدانی قرار می‌گیرد. جامعه مورد مطالعه کلیه پزشکان متخصص بیمارستان‌های آموزشی تخصصی شهر اصفهان بود که بر اساس جدول مورگان حجم نمونه ۲۲۰ نفر از آن‌ها به روش نمونه‌گیری در دسترس انتخاب شدند که پس از توزیع پرسشنامه‌ها ۱۸۱ نفر از آن‌ها به پرسشنامه‌های پژوهش پاسخ کامل دادند. قسمت اول پرسشنامه‌های جمع‌آوری‌شده مربوط به مشخصات فردی می‌پردازد و قسمت دوم آن شامل سه پرسشنامه تعهد سازمانی، ادراک از شدت و قطعیت مجازات‌ها و پرسشنامه قصد نقض امنیت اطلاعات می‌باشد که از مقالات چاپ‌شده در ژورنال‌های معتبر علمی اقتباس و بومی‌سازی شد. جهت سنجش ادراک افراد از عواقب افشای اطلاعات از پرسشنامه D'Arcy و همکاران (۲۱) اقتباس و مورد بومی‌سازی و هنجاریابی قرار گرفت. تعداد سؤالات این پرسشنامه ۷ ماده و دارای دو بعد درک از قطعیت مجازات‌ها و درک از شدت مجازات‌ها می‌باشد. جهت سنجش تعهد سازمانی، پرسشنامه تعهد سازمانی ۲۴ سؤالی Allen و Meyer (۱۸) مورد استفاده قرار گرفت. پرسشنامه حاضر دارای یک نمره کلی به عنوان تعهد سازمانی و سه خرده مقیاس تعهد عاطفی، تعهد هنجاری و تعهد مستمر می‌باشد.

شیوه نمره‌گذاری سؤالات غیر دموگرافیک، بر اساس طیف لیکرت ۵ درجه‌ای ۵ (کاملاً موافقم) تا ۱ (کاملاً مخالفم) می‌باشد. جهت روایی پرسشنامه از سه روش روایی محتوا (با بررسی پرسشنامه توسط اساتید و متخصصین این حوزه)، روایی صوری (با توزیع پرسشنامه در بین عده محدودی از جامعه هدف) و پس از جمع‌آوری داده‌ها با استفاده از روایی سازه با رویکرد تحلیل عامل تأییدی استفاده شد. پس از تأیید روایی و پایایی، مدل ارائه‌شده توسط نرم‌افزار SmartPLS و با رویکرد حداقل مربعات جزئی تحلیل شد.

۴. یافته‌ها

یافته‌ها در سه بخش داده‌های دموگرافیک، روایی سازه و پایایی و آزمون فرضیه‌ها گزارش شده‌اند.

۴-۱. نتایج دموگرافیک

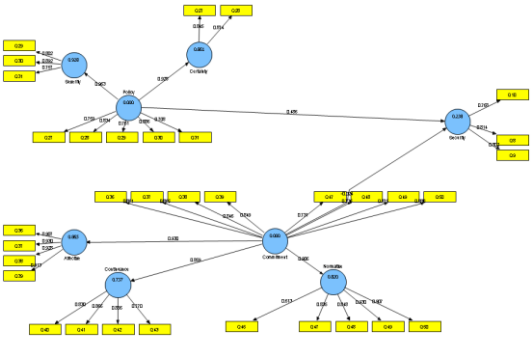
همانطور که در جدول ۱ نشان داده شده، بسیاری از پاسخ‌دهندگان مرد (۶۲/۹۸ درصد) در حالی که بزرگ‌ترین گروه از پاسخ‌دهندگان بین ۴۰-۳۱ سال (۴۶/۴۱ درصد) با ۱۵-۱۱ سال (۲۳/۲ درصد) سابقه کار بودند. یافته‌های مربوط به داده‌های دموگرافیک در جدول ۱ نمایش داده می‌شود.

جدول ۱: داده‌های دموگرافیک

ویژگی‌ها		فراوانی	درصد
جنسیت	مرد	۱۱۴	۶۲/۹۸
	زن	۶۷	۳۷/۰۲
سن	۳۰ و کم‌تر از ۳۰	۴۸	۲۶/۵۲
	۴۰-۳۱	۸۴	۴۶/۴۱
	۵۰-۴۱	۴۲	۲۳/۲۰
	بیشتر از ۵۰	۷	۳/۸۷
سابقه خدمت	کم‌تر از ۶ سال	۶۵	۳۵/۹۱
	۱۰-۶	۳۵	۱۹/۳۴
	۱۵-۱۱	۴۲	۲۳/۲۰
	۲۰-۱۶	۱۵	۸/۲۹
	۲۵-۲۱	۱۰	۵/۵۲
	بیشتر از ۲۵ سال	۱۴	۷/۷۳

۴-۲. روایی سازه و پایایی

از آنجا که اندازه نمونه کوچک‌تر از ۲۰۰ نفر بود و مدل دارای پیچیدگی (سازه دو بعدی) بود، از روش حداقل مربعات جزئی (PLS: Partial Least Square) و نرم‌افزار SmartPLS جهت تحلیل عامل تأییدی و آزمون فرضیه‌ها استفاده شد. بعد از سنجش اعتبار از این روش، گویه‌های ۲۶، ۳۵، ۶، ۷، ۴۴، ۳۲ و ۴۶ از مدل با توجه به بار عاملی پایین‌تر از استاندارد در متغیرها حذف شدند.



شکل ۱: نتایج تحلیل عامل تأییدی

همانطور که در شکل ۱ نشان داده شده، بار عاملی تمامی متغیرها بیش از ۰/۵ بر متغیرهای مربوط به خود را پیدا کردند. به علاوه همانطور که در جدول ۲ واریانس متوسط استخراج‌شده (AVE: Average Variance Extracted) بزرگ‌تر از ۰/۵ بود.

جدول ۲: نتایج پایایی و روایی

متغیرها	آلفای کرونباخ	CR	AVE
تعهد عاطفی	۰/۹۴	۰/۹۶	۰/۸۵
قطعیت مجازات	۰/۷۵	۰/۸۵	۰/۷۴
تعهد	۰/۹۴	۰/۹۵	۰/۶۹
تعهد مستمر	۰/۸۵	۰/۹۰	۰/۶۹
تعهد هنجاری	۰/۸۹	۰/۹۲	۰/۷۰
سیاست	۰/۸۵	۰/۸۹	۰/۶۳
امنیت	۰/۷۱	۰/۸۴	۰/۶۳
شدت مجازات	۰/۷۵	۰/۸۶	۰/۶۷

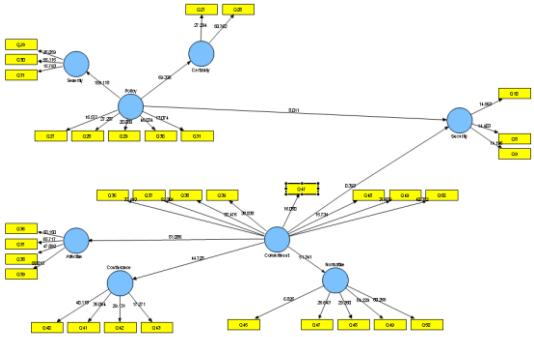
علاوه بر این، همانطور که در جدول ۳ نشان داده شده، مشخص شد که قاعده لارکر و فورنر رعایت شده است. برای تست قابلیت اطمینان از مقیاس قابلیت اطمینان پایایی مرکب (CR: Composite Reliability) و آلفای کرونباخ استفاده شد و همانطور که در جدول ۲ نشان داده شده است، پایایی مرکب و ارزش آلفای کرونباخ بیشتر از ۰/۷ نشان‌دهنده قابلیت اطمینان بالا برای مقیاس است. بنابراین نتایج حاکی است که مقیاس دارای روایی و پایایی قابل قبول است.

جدول ۳: قاعده لارکر و فورنر

متغیرها		میانگین	۱	۲	۳	۴	۵	۶	۷
۱	تعهد عاطفی	۰/۸۵							
۲	قطعیت مجازات	۰/۷۴	۰/۶۳						
۳	تعهد	۰/۶۹	۰/۶۷	۰/۵۲					
۴	تعهد مستمر	۰/۶۹	۰/۶۸	۰/۵۵	۰/۵۱				
۵	تعهد هنجاری	۰/۷۰	۰/۴۸	۰/۶۰	۰/۶۲	۰/۵۳			
۶	سیاست	۰/۶۳	۰/۶۲	۰/۵۶	۰/۳۵	۰/۵۹	۰/۴۲		
۷	امنیت	۰/۶۳	۰/۶۳	۰/۱۹	۰/۵۲	۰/۵۶	۰/۵۱	۰/۵۱	
۸	شدت مجازات	۰/۶۷	۰/۶۷	۰/۶۳	۰/۵۳	۰/۲۶	۰/۴۸	۰/۶۱	۰/۶۰

۴-۳. آزمون فرضیه‌ها

به منظور آزمون فرضیه‌ها از نرم‌افزار SmartPLS استفاده شد و همانطور که در جدول ۴ نشان داده شده، هیچ رابطه قابل توجهی بین شدت تعهد کارکنان و رعایت امنیت مشاهده نگردید، در حالی که مشخص شد که سیاست‌های سازمانی ادراک‌شده به طور قابل توجهی می‌تواند با رعایت امنیت در سازمان رابطه داشته باشد (P<0.001). جزئیات این آزمون فرضیه در شکل ۲ نشان داده شده است.



شکل ۲: نتایج فرضیه‌ها

جدول ۴: نتایج فرضیه‌ها

فرضیه	مقدار t	نتیجه فرضیه
رابطه تعهد با قصد نقض امنیت اطلاعات	۰/۳۹	رد شد
رابطه عواقب ادراک‌شده افشا با قصد نقض امنیت اطلاعات	۶۹/۳۳	پذیرفته شد

۵. بحث

مقاله حاضر با هدف تعیین رابطه ادراک پرسنل از عواقب افشای اطلاعات و تعهد کارکنان با قصد آن‌ها بر قصد نقض امنیت اطلاعات انجام گرفت. در فرضیه اول پژوهش ادراک پرسنل از سیاست‌های سازمانی که نشانگر قطعیت و شدت مجازات افشای اطلاعات است با در نظرگرفتن رابطه منفی بر قصد نقض امنیت اطلاعات بیماران توسط آن‌ها دارد، مورد بررسی قرار گرفت. نتایج به دست‌آمده حاکی از آن بود که در سطح معناداری (P<0.001) فرضیه حاضر مورد تأیید می‌باشد. نتایج پژوهش حاضر با نتایج به دست‌آمده از پژوهش‌های قبلی (۲۹-۲۱) همسو می‌باشد. در تبین یافته‌های حاضر می‌توان بیان داشت که زمانی که کارکنان نتایج رفتاری خود را مورد بررسی قرار دهند و با آن موضوع رو به رو شوند که برای عدم رعایت اصول امنیتی با مجازات‌هایی رو به رو می‌شوند، میل کم‌تری به انجام رفتارهای خطرآفرین در زمینه امنیت اطلاعات پیدا می‌کنند. به بیان دیگر زمانی که افراد نتایج رفتارهای خود را به وسیله عواقب ناشی از آن (تنبیه و مجازات

حتمی) ارزیابی می‌کنند، میل کم‌تری به نقض امنیت اطلاعات سازمان در آن‌ها به وجود می‌آید. همچنین می‌توان بیان کرد که هر چقدر که میزان اطمینان از دریافت مجازات‌ها بیشتر باشد، احتمال بروز رفتارهای مبنی بر سوءاستفاده از اطلاعات کاهش می‌یابد. کریمی و پیکری (۲۹) نشان دادند زمانی که در سیاست‌های امنیتی سازمان، عواقب افشای اطلاعات به طور واضح بیان شده باشد و کارکنان بداند که در صورت بروز رفتارهای نقض‌کننده امنیت اطلاعات با چه تنبیه‌هایی رو به رو خواهند شد، به صورت مثبت واکنش نشان داده و برای جلوگیری از تنبیه به سیاست‌های امنیتی سازمان پایبند خواهند بود، لذا قصد کم‌تری به نقض اصول امنیتی خواهند داشت.

در فرضیه دوم پژوهش مبنی بر ادراک پرسنل از تعهد عاطفی، هنجاری و مستمر تأثیر منفی معنادار بر قصد نقض امنیت اطلاعات بیماران توسط کارکنان، فرضیه پژوهش مورد تأیید قرار نگرفت و رد شد. نتایج پژوهش حاضر با نتایج پژوهش‌های (۱۴، ۳۳-۳۱) متناقض می‌باشد. در تبیین یافته‌های فوق می‌توان بیان نمود که از آنجایی نیروی انسانی یک سازمان بزرگ‌ترین ثروت و دارایی آن سازمان محسوب می‌شود و موفقیت سازمان‌ها در گروه وجود افرادی کارا و توانمند است که پیرو و تأثیرپذیر از سیاست‌ها و برنامه‌های سازمان خود بوده و خود را نسبت به اجرای آن‌ها متعهد بداند، چراکه کارایی و نوع ارزش‌ها و سیاست‌های حاکم بر سازمان است که باعث حرکت افراد در سازمان می‌باشد و تأثیر نافذی بر اجزای سازمان دارد، لذا اگر اعضای یک سازمان دارای اهداف، ارزش‌ها و سیاست‌های مشترکی باشند، در نهایت به آن‌ها دل‌بستگی عاطفی پیدا کرده و موجب می‌شود که نسبت به سازمان متعهد و وفادار بمانند (۳۴) و در نتیجه از سیاست‌های امنیتی و دستورات و برنامه‌های منطبق با آن پیروی کنند، ولی از آنجایی که چنین نتایجی یافت نشد، می‌توان بیان داشت که شدت و قطعیت سیاست‌ها و مجازات‌های تعیین شده برای نقض امنیت اطلاعات در سازمان مربوطه به اندازه کافی قدرت بازدارندگی از رفتارهای غیر منطبق با سیاست‌های سازمان را دارد و دیگر این‌که راه‌کارهای فنی جلوگیری از سوءاستفاده اطلاعات به مقدار کافی اثربخش می‌باشد. قصد سوءاستفاده از اطلاعات سازمان تحت تصرف عوامل گوناگونی قرار می‌گیرد که عوامل انگیزشی از مهم‌ترین آن‌ها می‌باشد. در نتیجه می‌توان گفت همانطور که برای شکل‌گیری و انجام رفتارهای سوءاستفاده از اطلاعات نیاز به انگیزه کافی وجود دارد، برای جلوگیری از آن نیز باید فرد از انگیزه کافی برخوردار باشد، لذا در زمینه حاضر می‌توان بیان کرد که اگر شدت رفتارهای بازدارنده و همچنین ادراک آن‌ها بیشتر از عوامل انگیزشی مؤثر در راه‌اندازی آن باشد، می‌تواند از بروز رفتار سوءاستفاده از اطلاعات سازمان مؤثر واقع شود. Barton و همکاران (۳۱) بیان می‌کنند که زمانی می‌توان کاربران یک سیستم را به خاطر نقض سیاست‌های امنیتی سازمان مورد بازرسی و توبیخ قرارداد که آن‌ها نسبت به عواقب رفتاری خودآگاهی کافی داشته باشند. به همین دلیل اعتقاد دارند اولین گام برای جلوگیری از سوءاستفاده از اطلاعات یک سازمان، فراهم‌سازی هوشیاری نسبت به شدت مجازات‌های تعیین‌شده برای رفتارهای نقض‌کننده حریم خصوصی و افشای اطلاعات به وسیله فرهنگ‌سازی سازمانی اتفاق می‌افتد. Chong و Eggleton (۳۲) جهت جلوگیری از رفتارهای مرتبط با نقض امنیت اطلاعات مدل تهدیدی را پیشنهاد می‌کنند. در مدل تهدید ارزیابی افراد از شدت مجازات‌های مطرح‌شده در مورد نقض امنیت اطلاعات باعث کاهش رفتارهای پرخطر و نقض‌کننده اصول امنیت اطلاعات می‌شود.

توجه مدیران و مسؤولان وزارت بهداشت به موضوع امنیت اطلاعات از جمله مواردی است که بر اساس تئوری بازدارنده رفتار تنظیم و تعیین می‌شود، پس چنانچه ارزیابی افراد از قطعیت و شدت مجازات‌های مربوط به عدم رعایت اصول امنیتی نادرست باشد و یا این‌که ادراکی در مورد شدت مجازات‌های مربوط به عدم رعایت اصول امنیت اطلاعات نداشته باشند، از سیاست‌های سازمان کم‌تر پیروی کرده و

رفتارهای پرخطر آن‌ها در مورد رعایت اصول امنیت اطلاعات بیماران بیشتر می‌شود، لذا در این زمینه پیشنهاد می‌شود در تعریف سیاست‌های سازمانی، رفتارهایی را که موجب نقض امنیت اطلاعات می‌شود را مشخص کنند تا کاربران بدانند چه رفتارهایی از نظر سازمان سوءاستفاده از اطلاعات تلقی می‌شود، عوامل انگیزشی مؤثر در زمینه شکل‌گیری رفتارهای سوءاستفاده عمدی از اطلاعات را شناسایی کنند تا بتوانند شدت تنبیه‌ها را به گونه‌ای تنظیم کنند که اثر بازدارندگی داشته باشد. همچنین پیشنهاد می‌شود جهت جلوگیری از سوءتفاهم در مورد سیاست‌های سازمانی، بایدها و نبایدها به صورتی صریح و واضح بیان شوند. همچنین با توجه به این‌که نتایج پژوهش حاضر رابطه معناداری بین تعهد سازمانی و مؤلفه‌های امنیت نشان نداد می‌توان نتیجه گرفت که قدرت سیاست‌های سازمانی در پیشگیری از سوءاستفاده از اطلاعات نقش بیشتری نسبت جهت حفظ امنیت اطلاعات سازمانی ایفا می‌کند، لذا پیشنهاد می‌شود برای تأیید یا رد این نتایج، پژوهش‌های مشابهی صورت گیرد. همچنین با توجه به این‌که روش پژوهش حاضر از نوع همبستگی می‌باشد، نمی‌توان از آن استنباط علت و معلولی کرد و همینطور به دلیل اجرای پژوهش حاضر در یک مؤسسه خدماتی در تعمیم نتایج آن به دیگر مؤسسات باید جانب احتیاط رعایت گردد.

۶. نتیجه‌گیری

یافته‌های این مطالعه مبین این مطلب است که چنانچه پرسنل نسبت به عواقب نقض و افشای اطلاعات محرمانه و حساس بیمار آگاهی‌های لازم را داشته باشند، از افشای این اطلاعات خودداری می‌کنند. عواقب افشای اطلاعات برای پرسنل می‌تواند شامل عواقب سازمانی مانند توبیخ، تعلیق، اخراج و یا عواقب قضایی مانند معرفی به مراجع قضایی جهت بررسی و تنبیه موارد افشای غیر قانونی اطلاعات محرمانه و حساس می‌باشد. بدیهی است مدیریت بیمارستان‌ها می‌تواند با در دستور کارگذاردن ابزار مناسب جهت اطلاع‌رسانی به پرسنل خود در این خصوص مانند برگزاری دوره‌ها و کلاس‌های آموزشی، ارسال پیامک ادواری به کارکنان و درج مطالب مرتبط در بولتن‌ها و نشریه‌های داخلی، نسبت به افزایش آگاهی پارکنان در این خصوص نقش به سزایی داشته باشند.

۷. تقدیر و تشکر

مقاله حاضر حاصل پایان‌نامه کارشناسی ارشد رشته مدیریت با کد ۲۳۸۲۱۲۱۰۹۶۲۰۰۵ و کد اخلاق IR.IAU.KHUISF.REC.1397.064 مصوب کمیته پژوهشی دانشکده مدیریت و معاونت پژوهشی دانشگاه آزاد اسلامی اصفهان (شعبه خوراسگان) می‌باشد. از حمایت دانشکده مدیریت و معاونت پژوهشی دانشگاه آزاد اسلامی اصفهان (شعبه خوراسگان) که در تصویب این مطالعه همکاری لازم را به عمل آورده و تمامی پرستارانی که در اجرای این پژوهش همکاری نمودند، تشکر و قدردانی می‌شود.

۸. سهم نویسندگان

نویسنده اول وظیفه تدوین اولیه ادبیات و جمع‌آوری اطلاعات را بر عهده داشت.

نویسنده دوم وظیفه ارائه مدل اولیه پژوهش، تحلیل مدل، نگارش و تدوین مقاله و پاسخ به داوری را بر عهده داشت.

۹. تضاد منافع

این مطالعه فاقد تضاد منافع بود.

References

1. Peikari HR, Zakaria MS, Norjaya MN, Hussain Shah M, Elhissi A. Role of CPOE usability in the reduction of prescribing errors. *Healthc Inform Res* 2013; 19(2): 93-101.

2. Hussain Shah M, Peikari HR. Usability and reduction of workload and medical errors; a survey amongst community physicians. *Telemedicine and e-Health* 2016; 2(1): 36-44.

3. Kuo A, Dang S. Secure Messaging in Electronic Health Records and Its Impact on Diabetes Clinical Outcomes: A Systematic Review. *Telemedicine and e-Health* 2016; 22(9): 125-132.

4. Luxton DD, Kayl RA, Mishkind MC. Health Data Security: The Need for HIPAA-Compliant Standardization. *Telemedicine and e-Health* 2012; 18(4): 124-131.

5. Fakhrzad M, Fakhrzad N, Dehghani M. The Role of Electronic Health Records in Presenting Health Information. *Media* 2012; 2(4): 31-40. [Persian]

6. Huffman E. Electronic Medical Record. Translated by Langarizadeh M. Tehran: Dibagaran; 2006.

7. Ghazi-Asgar M, Peikari HR, Ehteshami A. Health Information Management: Psychological factors influencing information privacy concerns in psychiatric hospitals. *Bali Medical Journal* 2018; 7(1): 1-7.

8. Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: A systematic literature review. *J Biomed Inform* 2013; 46(3): 541-562.

9. 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): 629-642.

10. Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, Sánchez-García AB, Hernández-Hernández 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): 454-467.

11. Khosravani M, Khosravani M, Rafiei F, Mohsenpour M. Organizational commitment and its dimensions in nurses working in Arak's hospitals. *Med Ethics J* 2017; 11(39): 37-44. [Persian]

12. Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* 2010; 34(3): 487-502.

13. Peikari HR, Ramayah T, Shah MH, Lo MC. Patients' perception of the information security management in health centers: The role of organizational and human factors. *BMC Med Inform Decis Mak* 2018; 18(1):102-122.

14. Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviours. *Computer & Security* 2005; 24(2): 124-133.

15. Lusignan SD, Chan T, Theadom A, Dhoul N. The roles of policy and professionalism in the protection of processed clinical data: a literature review. *Int J Med Inform* 2007; 76(4): 261-268.

16. Mahdad A. Industrial and Organizational Psychology. Tehran: Jangal Publisher; 2016. [Persian]

17. Sedaghatifard M, Khalaj Asadi SH. Relation with job satisfaction Index to organizational commitment in faculty members of Islamic Azad University-Garmsar Branch. *Journal of Modern Industrial/ Organization Psychology* 2011; 2(6): 39-51. [Persian]

18. Allen N, Meyer J. The measurement and antecedents of affective, continuance and normative commitment. *Journal of Occupational Psychology* 1990; 63(1): 1-18.

19. Ghayour Baghbani SM, Shojaei Kalate Bali N, Chenarani H, Ashoori J. The Relationship between Organizational Commitment, Job Satisfaction and Social Orientation, and the Nurses' Moral Behavior. *Med Ethics J* 2016; 10(37): 27-36. [Persian]

20. Zahed Babelan A, Khaleg Khah A, Kazemi S, Gharibzadeh R. The Role of Spiritual Leadership and Professional Ethics in Organizational Commitment of Health Care Workers. *Bioethics Journal* 2017; 7(26): 23-30. [Persian]

21. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 2009; 20(1): 79-98.

22. Albert L, Michelle M, Yair L. Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management* 2015; 3(1): 180-207.

23. Kruger HA, Kearney WD. A prototype for assessing information security awareness. *Computer & Security* 2006; 25(4): 289-296.

24. Sohrabi Safa N, Von Solms R, Furnell S. Information security policy compliance model in

organizations. *Computers & Security* 2016; 56: 70-82. [Persian]

25. Karami M, Safdari R, Soltani A. Patient's Information Rights: Strategies for Information Security in the Electronic Environment. *Medical ethics* 2013; 7(25): 83-96. [Persian]

26. 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. [Persian]

27. Elahi S, Taheri M, Hassanzadeh A. A framework for the role of human factors in information systems' security. *Management Research in Iran (Modares Human Sciences)* 2009; 13(2): 1-22. [Persian]

28. Kluge EHW. Secure e-health: managing risks to patient health data. *Int J Med Inform* 2007; 76(5): 402-406.

29. Karimi Z, Peikari HR. The Impact of Nurses' Perceived Information Security Training and Information Security Policy Awareness on their Perceived Severity and Certainty of Information Security Breach Penalties (Case: the Educational Specialized Hospitals of Isfahan City). *JNE* 2018; 7(2): 17-24. [Persian]

30. Waldo RF, Antonsen E, Ekstedt M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security* 2014; 43: 90-110.

31. Barton KA, Tejay G, Lane M, Terrell S. Information system security commitment: A study of external influences on senior management. *Computers & Security* 2016; 59: 9-25.

32. Chong VK, Eggleton IRC. The impact of reliance on incentive-based compensation schemes, information asymmetry and organisational commitment on managerial performance. *Management Accounting Research* 2007; 18(3): 312-342.

33. Koskosas I, Kakoulidis K, Siomos CH. Information Security: Corporate Culture and Organizational Commitment. *International Journal of Humanities and Social Science* 2011; 1(3): 1-12.

34. Ziaee MS, Roshandel Arbatani T, Nargesian A. Examine the relationship between organizational culture and organizational commitment among the staff of the library of Tehran University: Based on the Denison organizational culture model. *Journal of Academic Library and Information Science (LIS)* 2011; 45(1): 42-79. [Persian]

Faṣlnāmah-i akhlāq-i pizishkī
i.e., Quarterly Journal of Medical Ethics
2019; 13(44): e4
doi: https://doi.org/10.22037/mej.v13i44.19524
Journal Homepage: http://journals.sbmu.ac.ir/me

ORIGINAL RESEARCH **Open Access**

Information Security Management: The Impacts of Organizational Commitment and Perceived Consequences of Security Breach on the Intention of Patients' Information Security Violation

Zahra Karimi[1], Hamid Reza Peikari[2]*

1. MSc., Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran.
2 Assistant Professor, Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran. (Corresponding Author)

ARTICLE INFORMATION

Article history:
Received: *23 December 2017*
Accepted: *16 Febuary 2019*
Published online: *24 August 2019*

Keywords:
Organizational Commitment
Information Security Violation Intention
Security Policy

* **Corresponding Author: Hamid Reza Peikari**
Address: *Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran.*
Postal Box: 81595-158
Tel: *(+98) 3350 02729*
Email: omid726@yahoo.com

ABSTRACT

Background and Aim: Information security is a vital issue and nowadays, organizations all over the world have felt this fact. In the majority of the research conducted in this field, the role of human factor has been neglected and the past research has employed a technical approach to tackle this issue. The present article has been conducted with the aim of studying the impacts of personnel's perceptions about the consequences of sensitive information disclosure and personnel's organizational commitment on their intention to violate the information security.

Materials and Methods: The sample for this research was composed of 118 physicians, working in education specialized hospitals in Isfahan, who were non-randomly surveyed by using the scale adapted from D'Arcy et al. for security policy, including 7 items and Allen and Meyer for organizational commitment, including 24 items. After confirming its validity by face validity, content validity and construct validity, and its reliability by Cronbach's alpha and composite reliability, the hypotheses were examined by using partial least square technique, using SmartPLS.

Findings: The results of this study illustrated that physicians' perceptions toward organizational policies- which is an indication of certainty and severity of sanctions against unauthorized information disclosure has a negative impact on their intention to violate information security (P<0.001). Moreover, the results demonstrated that physicians' perceptions about the impact of organizational commitment, consisting of affective commitment, normative commitment, and continuance commitment had no significant impact on their intention to violate information security.

Ethical Considerations: Participation was voluntarily, participants' oral consent was obtained and their identity confidentiality was also assured.

Conclusion: Organizational policies in the sense of severity and certainty of the sanctions should be enhanced at the hospital and even ministry level and communicated with service providers in the health centers by using different tools.

Cite this article as: Karimi Z, Peikari HR. Information Security Management: The Impacts of Organizational Commitment and Perceived Consequences of Security Breach on the Intention of Patients' Information Security Violation. Faṣlnāmah-i akhlāq-i pizishkī i.e., Quarterly Journal of Medical Ethics. 2019; 13(44): e4.