Journal of Nursing Education (JNE) Original Article

June-July 2018, Volume 7, Issue 2 DOI: 10.21859/jne-07023

The Impact of Nurses' Perception of Information Security Training and Awareness of Information Security Policy on Their Perception of Severity and Certainty of Information Security Breach Penalties

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:** Hamid Reza Peikari, Assistant Professor, Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran. E-mail: omid726@yahoo.com

Received: 21 Dec 2017 **Accepted:** 12 Jun 2018

Abstract

Introduction: While nurses have access to confidential information of patients' records, it is still unknown that how information security training and awareness of information security policy can influence their perceived certainty and severity of sanctions. The current study aimed at examining the impact of nurses' perception of information security training and awareness of information security policy on their perception of severity and certainty of information security breach penalties in specialized teaching hospitals.

Methods: The current descriptive, correlational study was conducted on all the nurses working at specialized training hospitals of Isfahan, Iran as the study population and accordingly, 181 nurses were selected. The data were collected by four questionnaires as information security training developed by D'Arcy et al., security policy awareness developed by Sohrabi Safa et al., and perceived certainty and severity of sanctions developed by Cheng et al., scored based on a five-option Likert scale. The data were collected using non-random sampling. To assess the validity of the questionnaires, content, face, and construct validity, and to assess their reliability Cronbach's alpha were used. Descriptive statistics, including frequency and percentage were used to analyze data with SPSS version 19; the study hypotheses were analyzed by partial least squares regression with SmartPLS M2.0.

Results: The average for security training, security awareness, perceived certainty, and severity of sanctions were 3.78, 3.41, 3.63, and 3.18, respectively. Nurses' awareness of security policies had a positive and significant impact on their perceived severity ($t = 9.1$, $P < 0.01$, $\beta = 0.41$) and certainty ($t = 7.3$, $P < 0.01$, $\beta = 0.35$) of breach penalties. Training programs had also a significant impact on their perceived severity ($t = 2.3$, $P < 0.05$, $\beta = 0.37$) and certainty ($t = 2.8$, $P < 0.01$, $\beta = 0.44$) of breach penalties.

Conclusions: Security training and nurses' awareness of security policies can significantly predict their perceived certainty and severity of sanctions for security breach.

Keywords: Training, Nurses, Awareness of Security Policy, Certainty and Severity of Sanctions, Patients' Records

نشریه آموزش پرستاری | مقاله پژوهشی

خرداد و تیر ۱۳۹۷، دوره ۷، شماره ۲

DOI: 10.21859/jne-07023

تاثیر ادراک پرستاران از آموزش امنیت اطلاعات و آگاهی از سیاست¬های امنیت اطلاعات بر ادراک از شدت و قطعیت مجازات نقض امنیت اطلاعات

زهرا کریمی [۱]، حمیدرضا پیکری [۲،*]

[۱] کارشناسی ارشد، گروه مدیریت، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران

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

[*] **نویسنده مسئول**: حمیدرضا پیکری، استادیار، گروه مدیریت، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران.

ایمیل: omid726@yahoo.com

تاریخ دریافت مقاله: ۱۳۹۶/۱۰/۰۷ **تاریخ پذیرش مقاله:** ۱۳۹۷/۰۳/۲۲

چکیده

مقدمه: دسترسی گسترده پرستاران به اطلاعات محرمانه پرونده بیمار و همچنین عدم آگاهی پرستاران از اهمیت امنیت اطلاعات و نحوه محافظت از آنها، امنیت اطلاعات حساس بیماران را تهدید می کند. بنابراین نیاز به ارائه آموزشهای امنیت اطلاعات و همچنین ارتقاء آگاهی پرستاران در خصوص امنیت اطلاعات می باشد. مطالعه‌ی حاضر جهت تعیین تاثیر ادراک پرستاران از آموزش امنیت اطلاعات و آگاهی از سیاست‌های امنیت اطلاعات بر ادراک از شدت و قطعیت مجازات نقض امنیت اطلاعات در بیمارستان‌های تخصصی آموزشی انجام شده است.

روش کار: مطالعه حاضر، تحقیق توصیفی-همبستگی بود. جامعه پژوهش شامل پرستاران شاغل در بیمارستان‌های آموزشی تخصصی شهر اصفهان بودند که نهایتا ۱۸۱ پرسشنامه، جمع‌اوری شد. ابزارهای مورد استفاده، شامل چهارپرسشنامه‌ی بومی‌سازی شده، آموزش امنیت اطلاعات (D'Arcy و همکاران)، آگاهی از سیاست‌های امنیتی (Sohrabi Safa و همکاران) و قطعیت و شدت مجازات نقض امنیت اطلاعات (Cheng و همکاران) که در فرمت لیکرت طیف ۵ طراحی شده بود. آمار توصیفی شامل درصد و فراوانی توسط نرم افزار SPSS۱۹ و فرضیه‌ها با روش حداقل مربعات جزئی و نرم افزار SmartPLSتحلیل شد.

یافته‌ها: میانگین برنامه‌های آموزشی، آگاهی از سیاست‌های امنیت اطلاعات، شدت و قطعیت ادراک شده به ترتیب ۳/۷۸، ۳/۴۱، ۳/۶۳، ۳/۱۸ شد. برنامه‌های آموزشی تاثیر مثبت بر ادراک آنها نسبت به شدت (β = ۰/۳۷، P< ۰/۰۵، t =۲/۳) قطعیت مجازات (β = ۰/۴۴، P< ۰/۰۱، t =۸/۲) افشای اطلاعات دارد.آگاهی پرستاران از سیاست‌های امنیتی سیستم‌های اطلاعاتی تاثیر مثبت بر ادراک آنها نسبت به شدت (β = ۰/۴۱، P< ۰/۰۱، t =۱/۹) و قطعیت مجازات افشای اطلاعات (β = ۰/۳۵، P< ۰/۰۱، t =۳/۷) دارد.

نتیجه گیری: آموزش امنیت اطلاعات و ارتقاء آگاهی پرستاران از سیاست‌های امنیت اطلاعات بیمارستان بر ادراک پرستاران از شدت و قطعیت مجازات ناشی از نقض امنیت اطلاعات تاثیر دارد.

کلیدواژه‌ها: آموزش، آگاهی از سیاست امنیت اطلاعات، قطعیت و شدت مجازات، پرستاران، مستندات بیماران

مقدمه

در سال‌های اخیر با پیشرفت فنّاوری اطلاعات و ارتباطات، حوزه درمان شاهد به کارگیری تجهیزات الکترونیکی و روش‌های مجازی در بخش عمده‌ای از فعالیت‌های بیمارستان‌ها همچون ارائه خدمات درمانی، نظارت و اطلاع‌رسانی می‌باشد. ازطرف‌دیگر با رشد و توسعه فزاینده فنّاوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات افزایش‌یافته‌است و روش‌های اعمال تهدیدهای یادشده گسترده‌تر و پیچیده-تر می‌شود. ازآنجا که امنیت وکنترل اطلاعات سلامت مربوط به بیمار عاملی اساسی درتمام سیستم‌های اطلاعات سلامت است (۱)، در این رابطه، نگرانی

زیادی درمورد تأمین امنیت اطلاعات توسط پرسنل و کادر درمان به وجود آورده است؛ زیرا مدارک پزشکی بیمار شامل برخی از خصوصی‌ترین و محرمانه‌ترین اطلاعات بیمار بوده و با توجه با این‌که اطلاعات رایانه‌ای ازمکان‌های متعددی قابل دسترس است، به‌راحتی می‌تواند مورد سوء استفاده قرار گیرد. از این‌رو، حفظ امنیت تبادل اطلاعات از جمله مهمترین اهداف توسعه فنّاوری اطلاعاتی و ارتباطی محسوب می‌شود (۲). این درحالی است که در برنامه‌های امنیت اطلاعات،عامل انسانی اغلب به عنوان یکی از اصلی‌ترین عوامل محسوب می‌شوند (۳). یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقاء آگاهی و ادراک کاربران از امنیت اطلاعات است. دراین‌صورت، افراد آگاهی‌های لازم و مربوط به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می‌کنند (۴). براساس آنچه که گفته شد، یکی از جنبه‌های مهم در مدیریت امنیت اطلاعات در سازمان، توجه به امنیت ازمنظرمنابع انسانی است،بطوری‌که بدون درنظرگرفتن عوامل انسانی راه حل‌های فنی چندان تأثیر در مدیریت امنیت اطلاعات نخواهند داشت (۵) از جمله عوامل موثر عوامل انسانی در تامین امنیت اطلاعات، موضوع آگاهی و آموزش امنیت اطلاعات کاربران است (۶). ایندرحالی‌است که علی‌رغم طرح نقش آموزش امنیت اطلاعات به پرستاران درافزایش رفتار محتاطانه آنها جهت نقض امنیت اطلاعات در بیمارستان‌ها، محققان مطالعه‌ای که این رابطه را در میان پرستاران بسنجد، نیافتند که این امر بیانگر خلا تحقیقاتی در این حوزه می‌باشد. البته مطالعات متعددی در حوزه امنیت اطلاعات سلامت انجام شده (به عنوان مثال مطالعات (۷-۱۱))، در ایران، تنها مطالعه پیری و همکاران (۱۲) به بررسی وضعیت امنیت اطلاعات از دیدگاه پرستاران پرداخته است و دیگر مطالعات بر روی پرستاران متمرکز نشده‌اند. به‌علاوه، مطالعه فوق نیز صرفاً از روش پیمایشی در تحلیل داده‌ها استفاده کرده و عوامل موثر بر ادراک پرستاران از قطعیت و شدت عواقب نقض امنیت اطلاعات بیماران را نسنجیده، بلکه صرفاً عملکرد و وضعیت موجود امنیت اطلاعات سیستم اطلاعات بیمارستانی را از دیدگاه پرستاران گزارش کرده است. بنابراین نیاز به طراحی و اجرای یک مطالعه همبستگی جهت تعیین عوامل موثر بر ادراک پرستاران از قطعیت و شدت عواقب نقض امنیت اطلاعات بیماران ضروری به نظر می‌رسد.

اگر آگاهی وآموزش امنیت اطلاعات به عنوان بخشی از مشاغل درنظر گرفته شود، افراد نسبت به شغل و وظیفه خود احساس مسؤولیت می‌کنند (۵). در واقع یکی از بهترین راه‌های کاهش خطر امنیت اطلاعات در سازمان‌ها، آگاه سازی هرچه بیشتر کارمندان نسبت به مسائل امنیتی است. این آگاهی به این معنا است که آنها باید مسولیت اعمال خود در محیط کاری را به عهده گیرند (۱۳). تحقیقات نشان می‌دهد، قوانین و مجازات‌های تدوین شده، می‌تواند اعضای یک سازمان را از رفتار و تخلفات امنیتی برحذر دارد (۱۴). بنابراین، تدابیر قانونی زمانی قدرت بازدارندگی دارد که با ارائه آموزش و آگاهی از رفتارهای غیرقابل قبول و سپس ایجاد ترس و یا تمایل برای جلوگیری از پیامدهای منفی درک صحیحی ایجاد کند. از آن‌جا که سیاست‌های امنیتی معادل با قوانین سازمانی است، انتظار می‌رود، درک عواقب نقض قوانین سازمانی باعث کاهش رفتارهای مرتبط با افشای اطلاعات گردد، چرا که تدوین این تدابیر باعث افزایش آگاهی کارکنان از عواقب نقض امنیت اطلاعات می‌شود. این درحالی است که اگر سیاست روشن و درستی در زمینه مجازات افراد خاطی در نظر گرفته نشود، منجر به سهل‌انگاری کاربران در زمینه افشای اطلاعات و نقض امنیت اطلاعات می‌شود (۱۵). لذا در پژوهش حاضر، هدف آن است که تاثیر آموزش و آگاهی از سیاست‌های امنیتی سازمان را بر شدت و حتمیت ادراک شده مجازات نقض امنیت اطلاعات را بین پرستاران بیمارستان‌های تخصصی آموزشی شهر اصفهان مطالعه کند.

روش کار

روش تحقیق در این پژوهش، توصیفی از نوع همبستگی است و در زمره مطالعات میدانی قرار می‌گیرد. جامعه مورد مطالعه پرستاران رسمی (قطعی/ آزمایشی)، پیمانی و طرحی به تعداد ۵۳۹نفر شاغل در بیمارستان‌های آموزشی تخصصی شهر اصفهان بودند که 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 دادند. جهت رعایت اخلاق تحقیق، نخست شرکت در مطالعه و پاسخ به پرسشنامه‌ها اختیاری و داوطلبانه اعلام شد. همچنین پرستاران مجاز بودند، هر زمان اراده کردند از پاسخ به سوالات امتناع کرده و از مطالعه خارج شوند. درمرحله بعد، تضمین داده شده که هویت آنها و محتوای پاسخ هریک از آنها محرمانه نگه داشته شود. قسمت اول پرسشنامه ، مشخصات جمعیت‌شناختی و بخش بعدی پرسشنامه‌های خودگزارش‌دهی شامل ۱۶ سوال در چهار پرسشنامه بومی سازی شده آگاهی از سیاست های امنیتی (۱۶) قطعیت و شدت مجازات نقض امنیت اطلاعات (۱۷) و آموزش امنیت اطلاعات (۱۸) بر اساس طیف لیکرت ۵ درجه ای ۵ (کاملا موافقم) تا ۱ (کاملا مخالفم) بود. اندازه‌گیری میزان آگاهی پرستاران از سیاست‌های امنیت اطلاعات سازمان، از آنها در خصوص مطالبی مانند آشنایی آنها با سیاست‌های سازمان در خصوص دسترسی به کامپیوتر، دسترسی به اطلاعات، و روش‌های محافظت از کامپیوتر سوال شد. پرسش‌های مربوط به آموزش مواردی مانند ارائه آموزش‌های لازم به پرستاران جهت محافظت از امنیت اطلاعات، آموزش‌هایی در خصوص سیاست‌های امنیت اطلاعات سازمان و آموزش‌هایی در خصوص عواقب نقض امنیت اطلاعات را دربرمی‌گرفت. سوالات قطعیت مجازات نقض امنیت اطلاعات شامل پرسش‌هایی در خصوص آگاهی فرد از وجود تنبیه‌ها و مجازات‌های نقض اصول امنیت اطلاعات بود. پرسشنامه‌ی شدت مجازات نقض امنیت اطلاعات، مواردی مانند انتظار پاسخ دهنده را در خصوص شدت مجازات‌های نقض امنیت اطلاعات (برخوردهای شدید و اخراج از کار) می‌سنجد. تعداد دقیق سوالات هر پرسشنامه در جدول ۱ ذکر شده است. محدوده نمرات هر یک از پرسشنامه‌های آگاهی از سیاست‌های امنیتی و شدت ادراک شده مجازات بین ۴ تا ۲۰ می‌باشد. محدوده نمرات پرسشنامه‌های آموزش امنیت اطلاعات بین ۵ تا ۲۵ و قطعیت ادراک شده مجازات بین ۳ تا ۱۵ می‌باشد. نمره بالاتر در هر یک از این پرسشنامه‌ها، بیان‌گر وضعیت بهتر پاسخگو در هر یک از متغیرهای مورد مطالعه است. جزئیات گویه‌های مربوط به ۴ پرسشنامه فوق در قسمت ضمائم ارائه شده است. 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 جمع‌اوری داده‌ها با استفاده از روایی سازه با رویکرد تحلیل عامل تاییدی انجام شد. جهت بررسی روایی سازه از شاخص‌های متوسط واریانس استخراج شده (AVE: Average Variance Extracted) و بار عاملی استفاده شد. چنان‌که در جدول ۱ نشان داده شده، متوسط واریانس

استخراج شده از ۰/۵ بیشتر بود. به علاوه، بار عاملی تمام گویه‌ها از ۰/۵ بیشتر شد.

همچنین در جدول ۲ ذکر شده که،قاعده Fornel و Larcker رعایت شده. قاعده Fornel و Larcker برای ارزیابی روایی استفاده می شود. در این قاعده باید مجذور مقدار متوسط واریانس استخراج شده هر متغیر نهفته بیش از میزان همبستگی این متغیر با دیگر متغیرهای مدل باشد. ازان‌جاکه کلیه قواعد روایی در این مطالعه رعایت شده، در نتیجه روایی واگرا و همگرا تأیید شده که این خود بیان‌گر روایی مورد قبول سازه در این مطالعه می‌باشد. روایی همگرا یعنی بین گویه‌های که یک متغیر را می‌سنجند، همبستگی مناسبی وجود دارد، درحالی‌که روایی واگرا یعنی بین گویه‌های که متغیرهای متفاوت را می‌سنجند، همبستگی پایینی وجود دارد. همچنین، چنان‌که در جدول ۱ ذکر شده، آلفای کرونباخ برای هر یک از متغیرها بیش از ۰/۷ می‌باشد که بیانگر پایایی ابزار مورد استفاده می‌باشد. این مطالعه جهت آمار توصیفی از روش فراوانی و از نرم افزار SPSS 19 و جهت آزمون فرضیه‌ها از روش حداقل مربعات جزئی (PLS: Partial Least Square) و نرم‌افزار SmartPLS .0 استفاده کرده است. روش حداقل مربعات جزئی یکی از تکنیک‌های معادلات ساختاری (SEM: Structural Equation Modelling) می‌باشد. این روش ترکیبی از روایی سازه به روش تحلیل عامل تاییدی، تحلیل مسیر و رگرسیون می‌باشد که جهت تحلیل مدل‌های همبستگی پیچیده که دارای تعداد نمونه اندک یا توزیع غیر نرمال داده‌ها، استفاده می‌شود.علت استفاده از این روش جهت تحلیل فرضیه‌ها، این است که اولاً نوع مطالعه از نوع همبستگی بوده و محققان سعی در آزمودن تاثیر متغیرها بر یکدیگر با استفاده از تحلیل مسیر داشته‌اند. ثانیاً این روش هم‌زمان نتایج تحلیل عامل تاییدی را نیز برای محقق مهیا می‌سازد. به علاوه از آن‌جا که مدل دارای پیچیدگی بوده و دارای دو متغیر وابسته بوده و مدل توسط رگرسیون ساده قابل سنجش نبود، بنابراین از روش حداقل مربعات جزئی برای سنجش فرضیه‌ها استفاده شد.

یافته ها

شامل دو دسته نتایج جمعیت‌شناختی و نتایج فرضیه‌ها است. همان‌طور که در جدول۳ نشان داده شده، بسیاری از پاسخ‌دهندگان مرد (۶۲/۹۸٪) درحالی که بزرگ‌ترین گروه از پاسخ‌دهنده‌ها بین ۳۱-۴۰ سال (۴۶/۴۱٪) با ۱۱-۱۵ سال (۲۳/۲٪) سابقه کار بودند.

جدول ۱: منابع پرسشنامه، روایی و پایایی

متغیرها	تعداد سوالات	منبع	آلفای کرونباخ	AVE
آگاهی از سیاست‌های امنیتی	۴	Sohrabi Safa و همکاران (۱۰)	۰/۸۱	۰/۶۰
آموزش امنیت اطلاعات	۵	D'Arcy و همکاران (۱۱)	۰/۸۰	۰/۵۹
قطعیت ادراک شده مجازات	۳	Cheng و همکاران (۱۲)	۰/۸۶	۰/۵۹
شدت ادراک شده مجازات	۴	Cheng و همکاران (۱۲)	۰/۷۶	۰/۷۲

جدول ۲: قاعده لارکر و فورنر

متغیرها	۱	۲	۳	۴
آگاهی از سیاست امنیتی	۰/۶۰۵			
آموزش	۰/۳۵۹	۰/۵۹۲		
قطعیت مجازات	۰/۳۳۵	۰/۳۳۷	۰/۵۹۱	
شدت مجازات	۰/۳۳۳	۰/۲۱۲	۰/۴۲۵	۰/۷۲۵

جدول۳: نتایج تحلیل جمعیت شناختی

طبقه	فراوانی	درصد
جنسیت		
مرد	۱۱۴	۶۲/۹۸
زن	۶۷	۳۷/۰۲
سن		
۳۰ و کمتر از ۳۰	۴۸	۲۶/۵۲
۳۱-۴۰ سال	۸۴	۴۶/۴۱
۴۱-۵۰ سال	۴۲	۲۳/۲
بیشتر از ۵۰	۷	۳/۸۷
سابقه خدمت		
کمتر از ۶ سال	۶۵	۳۵/۹۱
۶-۱۰ سال	۳۵	۱۹/۳۴
۱۱-۱۵ سال	۴۲	۲۳/۲
۱۶-۲۰ سال	۱۵	۸/۲۹
۲۱-۲۵ سال	۱۰	۵/۵۲
بیشتر از ۲۵ سال	۱۴	۷/۷۳

جدول ۴: میانگین امتیاز متغیرها

متغیرها	میانگین امتیاز
آگاهی از سیاست امنیتی	۳/۴۱
آموزش	۳/۷۸
قطعیت مجازات	۳/۱۸
شدت مجازات	۳/۶۳

جدول ۵: نتایج فرضیه‌ها، ضریب مسیر، مقدار t و مقدار P

فرضیه‌ها	ضریب مسیر	مقدار t	مقدار P	نتیجه
آگاهی از سیاست امنیتی -> شدت مجازات	۰/۴۱	۹/۱	P < ۰/۰۱	تایید
آگاهی ازسیاست امنیتی -> قطعیت مجازات	۰/۳۵	۷/۳	P < ۰/۰۱	تایید
آموزش -> شدت مجازات	۰/۳۷	۲/۳	P < ۰/۰۱	تایید
آموزش -> قطعیت مجازات	۰/۴۴	۲/۸	P < ۰/۰۱	تایید

در جدول ۴ میانگین امتیاز هر یک از متغیرها ذکر شده است. طبق این جدول، آموزش بیشترین میانگین امتیاز را و قطعیت مجازات کمترین میانگین امتیاز را به خود تخصیص داده‌اند. در جدول ۵ خلاصه ضرایب مسیر و معنی داری روابط نشان داده شده است. نتایج تحلیل معادله ساختاری نشان می‌دهد که تاثیر آگاهی از سیاست‌های امنیتی بر شدت مجازات (β = ۰/۴۱، P < ۰/۰۱، t = ۹/۱) و قطعیت مجازات افشای اطلاعات (β = ۰/۳۵، P < ۰/۰۱، t = ۷/۳) با معناداری ۰/۹۹ مورد تایید است. همچنین با توجه به مقدار ضریب استاندارد شده، می توان گفت این متغیر توانسته ۰/۳۵ از تغییرات در ادراک پرستاران از قطعیت مجازات نقض امنیت اطلاعات و ۰/۴۱ از تغییرات در ادراک پرستاران از شدت مجازات نقض امنیت اطلاعات را تبیین کند. همچنین نتایج نشان می‌دهد که تاثیر آموزش‌های امنیت اطلاعات بر شدت مجازات (β = ۰/۳۷، P < ۰/۰۵، t = ۲/۳) در سطح ۰/۹۵ و بر قطعیت مجازات افشای اطلاعات (β = ۰/۴۴، P < ۰/۰۱، t = ۲/۸) با معناداری ۰/۹۹ مورد تایید است. همچنین با توجه به مقدار ضریب استاندارد شده، می‌توان گفت، آموزش امنیت اطلاعات به پرستاران توانسته۰/۴۴ از تغییرات در ادراک پرستاران از قطعیت مجازات نقض امنیت اطلاعات و ۰/۳۷ از تغییرات در ادراک پرستاران از شدت مجازات نقض امنیت اطلاعات را تبیین کند. در مجموع، می‌توان گفت تمام روابط مدل تایید شد و آموزش امنیت اطلاعات و آگاهی از سیاست‌های امنیت اطلاعات بر ادراک پرستاران از قطعیت و شدت مجازات نقض امنیت تاثیر معنادار دارند.

بحث

نتایج تحلیل آماری نشان داد، برنامه‌های آموزشی پرستاران بیمارستان‌های تخصصی شهراصفهان، تاثیر مثبت معناداری بر ادراک آنها نسبت به شدت (P < ۰/۰۵) و قطعیت مجازات (P < ۰/۰۱) افشای اطلاعات دارد. آگاهی پرستاران از سیاست‌های امنیتی سیستم‌های اطلاعاتی تاثیر مثبت معنادار بر ادراک آنها نسبت به شدت (P < ۰/۰۱) و قطعیت مجازات افشای اطلاعات (P < ۰/۰۱) دارد. در تبیین این یافته‌ها می‌توان، بیان داشت که قوانین و مجازات‌های قانونی می‌تواند پرستاران را از درگیر شدن در رفتارهای غیرقانونی دل‌سرد کند. از آن‌جاکه تدابیر امنیتی معادل قوانین سازمانی می‌باشند، انتظار می‌رود این تدابیر به عنوان یک مکانیزم بازدارنگی در نقض امنیت اطلاعات عمل کنند. لذا تدابیر و سیاست‌های امنیتی بیمارستان پایه‌ای برای بازرسی و دادخواهی خواهد شد که ببراساس آن نحوه‌ی مجازات پرستاران خاطی مشخص می‌شود. برخی محققان اعتقاد دارند زمانی تعهد افراد نسبت به رعایت اصول امنیت اطلاعات افزایش می‌یابد که بدانند برای رفتارهای نامنطبق با اصول امنیت اطلاعات سازمان بطور اخص و با سیاست‌های سازمانی به‌طورکلی عواقب و مجازات‌هایی درنظرگرفته شده است (۱۹). برخی محققان به این موضوع اشاره می‌کنند که سیاست‌های امنیت اطلاعات سازمان با روشن کردن موارد نقض امنیت و نوع مجازات‌های مرتبط با آن، باعث شکل‌گیری اعتقادات هنجاری و نگرش‌های مرتبط با سازمان در جهت پیروی از رعایت اصول امنیت اطلاعات می‌شوند (۲۰). بنابراین می‌توان، نتیجه گرفت، وقتی که پرستاران از سیاست‌های امنیتی سازمان اطلاع کامل داشته باشند،عواقب ناشی از رفتارهای نقض کننده این سیاست‌ها را می‌دانند و به همین خاطر برای جلوگیری از تنبیه و مجازات وضع شده انگیزه بیشتری نسبت به رعایت اصول امنیتی دارند. به‌عبارت دیگر، وقتی نگرش پرستاران نسبت به سیاست‌های امنیتی سازمان روش و دقیق است که بدانند در قبال تخطی از این سیاست‌ها، چه عواقبی در انتظار آن‌ها است. از طرفی، از آن‌جایی که قوانین و تدابیر امنیتی وضع شده توسط بیمارستان‌ها عاملی برای برخورد آنها در برابر رفتارهای نقض کننده امنیت می‌باشد، بنابراین زمانی که پرستاران متوجه مجازات‌های وضع شده در برابر رفتارهای نقض کننده امنیت اطلاعات شوند و از شدت آنها آگاهی لازم را به دست آورند، انگیزه بیشتری برای رعایت این اصول و قوانین پیدا می‌کنند و برای جلوگیری از روبرو شدن با مجازات‌های وضع شده توسط بیمارستاران، خود را متعهد به رعایت اصول امنیتی سازمان می‌دانند. Herath و Rao (۱۹) اعتقاد دارند که ادراک کارکنان مبنی بر پایین بودن شدت مجازات‌ها باعث افزایش رفتارهای پر خطر در مورد رعایت اطلاعات می‌شود. یعنی چنان‌چه، کارکنان سازمانی شدت مجازات‌های مربوط به عدم پیروی از سیاست‌های امنیتی سازمان را کم شدت و گذرا ادراک کرده، به همان میزان،رعایت رفتارهای امنیتی نیز کاهش می‌یابد. در تبیین این فرضیه، می‌توان بیان کرد که پرستاران بر اساس تئوری بازدارنده[1]،

[1] Deterrence Theory: یکی از نظریه های مطرح در مطالعات حوزه مطالعات جرم شناسی و بازدارندگی و کاهش تمایل افراد برای بروز رفتار مجرمانه و از جمله نقض امنیت اطلاعات می باشد که شامل دو بعد قطعیت و شدت مجازات رفتار مجرمانه می باشد (۸، ۱۱). این به این معناست که به عنوان مثال در حوزه امنیت اطلاعات، در صورتیکه کارمندان معتقد باشند که در صورت نقض امنیت اطلاعات در سازمان، مجازات آنها قطعی و شدید خواهد بود، تمایل کمتری به بروز این رفتار خواهند داشت.

رفتارهای خود را تنظیم و تعیین می‌کنند. چنان‌چه ارزیابی پرستاران از شدت مجازات‌های مربوط به عدم رعایت اصول امنیتی نادرست باشد و یا این‌که ادراکی در مورد شدت مجازت‌های مربوط به عدم رعایت اصول امنیت اطلاعات نداشته باشند، از سیاست‌های بیمارستان کمتر پیروی کرده و رفتارهای پرخطر آنها در مورد رعایت اصول امنیت اطلاعات بیماران بیشتر می‌شود. برخی محققان (۲۱) پیشنهاد می‌کنند، زمانی که به کاربران در مورد چگونگی استفاده از اطلاعات محرمانه و سیستم‌های اطلاعاتی آموزش داده شود و آنها نسبت به رفتارهای خطرآفرین و روش‌های ایجاد امنیت، اطاعات و آموزش کافی دریافت کنند، نسبت به رفتارهای پرخطر بینش کافی به دست آورده و از رفتارهای نقض کننده امنیت اطلاعاتی آنها کاسته می‌شود. در واقع وقتی-که بیمارستان‌ها محتوی اطلاعات طبقه‌بندی و محرمانه و رفتارهایی را که باعث افزایش احتمال نقض امنیت اطلاعات پرونده‌های بیماران خود می‌شود، را به همراه مجازات‌های تعیین شده برای پرستاران خود توضیح می‌دهند، دانش و آگاهی پرستاران را نسبت به آنچه باید انجام دهند و آنچه باید از انجام آن پرهیز کنند، را افزایش می‌دهند. به بیان دیگر، وقتی‌که پرستاران بدانند که بیمارستان در قبال اطلاعات محرمانه خود چه انتظاری از آنها دارد و همچنین روش‌های مورد قبول بیمارستان در مورد رعایت این اطلاعات چیست، ومتوجه میزان اهمیت این اطلاعات و روش‌های جلوگیری از سوء استفاده آنها شوند، درمی‌یابند که نقض این توقعات سازمانی با تنبیه‌ها و مجازات‌هایی همراه است، لذا در این زمان رفتارهای امنیتی آنها افزایش یافته و به شکل متعهدانه-ای به رعایت اصول امنیت اطلاعات می می‌پردازند. در مطالعات مشابهی، D'Arcy و همکاران (۱۸) گزارش دادند که آموزش‌های امنیت اطلاعات و ارتقاء آگاهی کارمندان سازمان‌ها نسبت به امنیت اطلاعات بر ادراک آنها از حتمیت و قطعیت مجازات‌ها تاثیر دارد. به همین ترتیب، Sohrabi Safa و همکاران (۲۲) نیز در مطالعه‌ای مشابه، گزارش کردند که آگاهی از برنامه‌های امنیت سازمان، بر نگرش پرسنل نسبت به امنیت اطلاعات تاثیر خواهد داشت که متعاقباً منجر به رفتارمحتاطانه آنان خواهد شد. از طرفی، مطالعه دیگری (۲۳) توصیه به ارتقاء آگاهی از امنیت اطلاعات و آموزش امنیت اطلاعات در بین پرسنل جهت ارتقاء امنیت اطلاعات نموده است.

نتیجه گیری

طبق یافته‌های مطالعه حاضر، آموزش پرستاران جهت ارتقاء سطح آگاهی و ادراک آنان از قطعیت و شدت وجود مجازات‌ها رفتارهای نقض کننده امنیت اطلاعات و ازجمله، عواملی است که باعث پیشگیری از انجام رفتارهایی می‌شود که به امنیت اطلاعات محرمانه بیمارستان آسیب وارد می‌کند. طبق یافته‌های مطالعه حاضر، آموزش سیاست‌های امنیت اطلاعات و آشنا ساختن پرستاران با سیاست‌های سازمان در خصوص امنیت اطلاعات می‌تواند نقش ویژه‌ای درافزایش حساسیت پرستاران در خصوص قطعیت و شدت عواقب نقض امنیت اطلاعات و نهایتاً بازداشتن آنها از نقض امنیت اطلاعات موجود در پرونده سلامت بیمار داشته باشد. بنابراین مقتضی است مسئولان حوزه درمان برنامه‌های آموزشی مناسبی را در دوران تحصیل و اشتغال پرستاران جهت ارتقای آگاهی پرستاران در خصوص سیاست‌های امنیت اطلاعات و عواقب نقض امنیت اطلاعات برگزار کنند. از آن‌جایی که آگاهی افراد از رفتارهای غیرقانونی، تاثیر چشم‌گیری در رعایت اصول مرتبط با قانون دارد و از آن‌جایی که این برنامه بر نوع و شدت مجازات‌های ناشی از عدم رعایت آن استوار است، می‌تواند تاثیری به‌سزایی در رعایت اصول امنیت اطلاعات توسط کاربران داشته باشد. برنامه‌های آموزشی و افزایش آگاهی پرستاران در مورد رعایت اصول امنیت اطلاعات باید در دو بعد دانش فنی در مورد چگونگی حفاظت و امنیت اطلاعات و همچنین میزان تحریم‌ها و مجازات‌های ناشی از عدم رعایت اصول امنیتی در بیمارستان باشد. زمانی‌که پرستاران از شدت مجازات‌های تعیین شده برای نقض اصول امنیتی آگاهی بیشتری داشته باشند، انگیزه بیشتری در زمینه استفاده از اصول امنیتی پیدا می کنند، که از این میان می‌توان به انتخاب رمزهای عبور مناسب و رعایت دیگر اصول مرتبط کار با سیستم‌های اطلاعاتی اشاره کرد. درحقیقیت، آموزش سیاست‌های مرتبط به رعایت اصول امنیتی وقتی اهمیت پیدا می کند که پرستاران برای رعایت آنها انگیزه کافی داشته باشند؛ این انگیزه زمانی به دست می‌آید که آنها از شدت مجازات‌های مطرح شده در مورد عدم رعایت اصول امنیتی سازمان آگاهی پیدا کنند. لذا چنین نتیجه گرفته می‌شود که، وقتی پرستاران خود را متعهد به رعایت اصول امنیتی در چارچوب برنامه-های آموزشی و افزایش آگاهی می‌دانند که انگیزه کافی برای انجام این رفتارها داشته باشند و این انگیزه حاصل نمی‌شود مگر زمانی که پرستاران نه تنها نسبت به وجود و قطعیت مجازات‌های وضع شده توسط بیمارستان آگاهی یابند، بلکه از شدت این مجازات‌ها نیز آگاه باشند. چنان‌که پیش‌تر نیزبیان شد، محققان مطالعه‌ای که، سعی در تعیین عوامل موثر بر ادراک پرستاران از قطعیت و شدت نقض امنیت اطلاعات کرده باشد، نیافتند و بنابراین این مطالعه از لحاظ بررسی تاثیر آموزش امنیت اطلاعات در قطعیت و شدت ادراک شده مجازات نقض امنیت اطلاعات در بین پرستاران دارای نو آوری نظری می‌باشد. پیام اصلی این پژوهش عبارت است از این-که ارائه آموزش نکات امنیت اطلاعات و ارتقاء آگاهی پرستاران در خصوص سیاست‌های امنیت اطلاعات بیمارستان موجب افزایش حساسیت پرستاران در خصوص قطعیت و شدت عواقب نقض امنیت اطلاعات می‌شود. باایان وجود، مانند دیگر مطالعات، این تحقیق نیز عاری از محدودیت نیست. محدودیت اول در خصوص استفاده از پرسشنامه و روش نمونه‌گیری در دسترس جهت جمع‌اوری داده‌ها است، پیشنهاد می‌شود روش‌های دیگر جمع‌آوری داده‌ها و نمونه-گیری جهت افزایش دقت نتایج و ارتقاء تعمیم‌پذیری داده‌ها استفاده شود. همچنین، نتایج این مطالعه در خصوص پرستاران شاغل در بیمارستان‌های آموزشی تخصصی اصفهان، قابل تعمیم است و از تعمیم آن در بین دیگر گروه‌های خدمات درمانی یا دیگر بیمارستان‌ها باید اجتناب نمود. محدودیت دیگر، در خصوص رویکرد این تحقیق در مفهوم‌سازی و سنجش متغیر آموزش امنیت اطلاعات است. پیشنهاد می‌شود، مطالعات آتی تاثیر روش‌های مختلف آموزش امنیت اطلاعات را(مانند آموزش کوتاه مدت/بلند مدت، آموزش حضوری/غیر حضوری، مستمر/غیرمستمر و ....) بر عواقب ادراک شده نقض امنیت اطلاعات، بی‌ازمایند. همچنین پیشنهاد می‌شود، مطالعات آتی، نقش آموزش امنیت اطلاعات را بر فرهنگ امنیتی و قصد رعایت/نقض امنیت اطلاعات مورد سنجش قرار دهند. پیشنهاد پژوهشی دیگر می-تواند درخصوص بررسی و مقایسه کارآیی آموزش‌های رسمی و متمرکز با آموزش‌های

غیررسمی و غیرمتمرکز در رابطه با مباحث رعایت امنیت اطلاعات و حریم خصوص بیماران توسط پرستاران طراحی شود.

سپاسگزاری

مقاله حاضر، منتج از پایان نامه کارشناسی‌ارشد رشته مدیریت با کد ۲۳۸۲۱۲۱۰۹۳۲۰۵۴ مصوب کمیته پژوهشی دانشکده مدیریت و معاونت آپژوهشی دانشگاه آزاد اسلامی اصفهان (شعبه خوراسگان) می‌باشد. ازحمایت دانشکده مدیریت و معاونت پژوهشی دانشگاه آزاد اسلامی اصفهان (شعبه خوراسگان) که در تصویب این مطالعه همکاری لازم را به عمل آورده وهمچنین کلیه بیمارستان‌های تخصصی-آموزشی شهر اصفهان و همه پرستارانی که در اجرای این تحقیق همکاری نمودند، تشکر و قدردانی می‌شود.

ضمیمه ۱: سوالات آگاهی از سیاست امنیتی، آموزش، ادراک ازقطعیت مجازات‌ها، ادراک از شدت مجازات‌ها

سوالات	کاملا مخالفم	مخالفم	نه مخالفم نه موافقم	موافقم	کاملا موافقم
آگاهی از سیاست امنیتی					
این بیمارستان دارای سیاست‌ها و دستورالعمل‌های خاص و قابل قبول برای کار با کامپیوتر دارد.					
در بیمارستان من قواعد و قانون‌هایی برای استفاده از منابع کامپیوتری وضع شده است.					
بیمارستان من دارای یک‌سری سیاست‌های رسمی می‌باشد که دسترسی پرستاران را به سیستم‌های اطلاعاتی که مجاز به استفاده از آن نمی‌باشند را منع می‌کند.					
بیمارستان من دارای دستورالعملهای خاصی برای مجاز کردن ارتباط پرستاران با کامپیوتر می‌باشد.					
آموزش					
بیمارستان، آموزش‌های لازم را برای کمک به بهبود آگاهی پرستاران از کامپیوتر و مسائل امنیتی فراهم می‌کند.					
بیمارستان، آموزش لازم در قوانین کپی رایت نرم افزارهای کامپیوتری را به پرستاران خود می‌دهد.					
در بیمارستان من، پرستاران در مورد عواقب دست‌کاری و سوءاستفاده از داده‌های کامپیوتری آگاهی‌های لازم را دارند.					
بیمارستان من، پرستاران خود را در مورد مسئولیت‌های امنیتی خود آموزش می‌دهد.					
در سازمان من، کارمندان در مورد عواقب ناشی از دسترسی به سیستم‌های اطلاعاتی که مجاز به استفاده از آنها نیستند،آگاهی‌های لازم را دارند.					
ادراک ازقطعیت مجازات ها					
من پس از نقض امنیت اطلاعات بیمارستان در نهایت گرفتار خواهم شد.					
من پس از نقض امنیت اطلاعات بیمارستان قطعا توسط مدیریت مواخذه خواهم شد.					
بیمارستان قوانین متقن و محکمی در خصوص نقض امنیت اطلاعات دارد که می تواند باعث جلوگیری از نقض اطلاعات گردد.					
ادراک از شدت مجازات ها					
اگر امنیت اطلاعات را نقض کنم به شدت مواخذه خواهم شد.					
اگر امنیت اطلاعات را نقض کنم مجازات من شدید خواهد بود.					
بیمارستان کارکنانی که دفعات به نقض قوانین امنیتی پرداخته اند را از کار اخراج می کند.					
اگر امنیت اطلاعات را نقض کنم دچار عواقب حقوقی و کیفری شدیدی خواهم شد.					

References

1. Faroukhzad M, Farokhzad N, Dehghani M. [The role of electronic records on the delivery of health information]. Univ Learn J. 2011;2:28-36.
2. Da Veiga A, Eloff JHP. A framework and assessment instrument for information security culture. Comp Secur. 2010;29(2):196-207. DOI: 10.1016/j.cose.2009.09.002
3. Ortega Egea JM, Román González MV. Explaining physicians' acceptance of EHCR systems: An extension of TAM with trust and risk factors. Comp Hum Behav. 2011;27(1):319-32. DOI: 10.1016/j.chb.2010.08.010
4. Van Niekerk JF, Von Solms R. Information security culture: A management perspective. Comp Secur. 2010;29(4):476-86. DOI: 10.1016/j.cose.2009.10.005
5. Dang-Pham D, Pittayachawan S, Bruno V. Exploring behavioral information security networks in an organizational context: An empirical case study. J Inf Secur Appl. 2017;34:46-62. DOI: 10.1016/j.jisa.2016.06.002
6. Shaw RS, Chen CC, Harris AL, Huang H-J. The impact of information richness on information security awareness training effectiveness. Comp Educ. 2009;52(1):92-100. DOI: 10.1016/j.compedu.2008.06.011
7. Arab M, Pourreza A, Eshraghian M, Khabiri R. Survey on Current Status of Patient Information Privacy in Tehran's Hospitals, Iran. Health Inf Manage. 2011;8(1):44-52.
8. Mehraeen E, Ayatollahi H, Ahmadi M. A study of information security in Hospital Information Systems. Health Inf Manage. 2014;10(6):779-88.
9. Z M, MA A, SG M, A A-A. Evaluation of Hospital Information Systems Security. Health Inf Manage. 2017;14(5):187-93.
10. Kahouei M, Abbasi Z. The Prioritization of Effective Factors on Electronic HealthInformation Security in Medical Centers. Health Inf Manage. 2015;12(2):170-82.
11. Sheikh Abumasoudi R, Koohi Habibi S, Ataei M, Esmaeili N. Evaluation of Information Management Systems in Isfahan University of Medical Science by ISO/IEC 27001 Standard. Health Inf Manage. 2015;12(33):316-26.
12. Piri Z, Naser S, KHezri H, Damnabi S. Investigating the functional model ehr security safeguards in the his of tabriz university of medical sciences. J Urmia Nurs Midwifery Fac. 2014;12(8):606-12.
13. von Solms R, von Solms B. From policies to culture. Comp Secur. 2004;23(4):275-9. DOI: 10.1016/j.cose.2004.01.013
14. Silic M, Barlow JB, Back A. A new perspective on neutralization and deterrence: Predicting shadow IT usage. Inf Manage. 2017;54(8):1023-37. DOI: 10.1016/j.im.2017.02.007
15. Rocha Flores W, Antonsen E, Ekstedt M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Comp Secur. 2014;43:90-110. DOI: 10.1016/j.cose.2014.03.004
16. Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. Comp Secur. 2015;53:65-78. DOI: 10.1016/j.cose.2015.05.012
17. Cheng L, Li Y, Li W, Holm E, Zhai Q. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Comp Secur. 2013;39:447-59. DOI: 10.1016/j.cose.2013.09.009
18. D'Arcy J, Hovav A, Galletta D. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Inf Syst Res. 2009;20(1):79-98. DOI: 10.1287/isre.1070.0160
19. Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Dec Support Syst. 2009;47(2):154-65. DOI: 10.1016/j.dss.2009.02.005
20. Bulgurcu, Cavusoglu, Benbasat. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Q 2010;34(3):523. DOI: 10.2307/25750690
21. Halibozek EP, Kovacich GL. Security Education and Awareness Training. 2017:249-74. DOI: 10.1016/b978-0-12-804604-3.00012-8
22. Sohrabi Safa N, Von Solms R, Furnell S. Information security policy compliance model in organizations. Comp Secur. 2016;56:70-82. DOI: 10.1016/j.cose.2015.10.006
23. Furnell S, Khern-am-nuai W, Esmael R, Yang W, Li N. Enhancing security behaviour by supporting the user. Comp Secur. 2018;75:1-9. DOI: 10.1016/j.cose.2018.01.016