فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Spring, 2022, 3 (1), 25-35
DOR: 20.1001.1.27832570.1400.2.4.5.2

Rcceived:15 March2022
Accepted: 28 Apr 2022

The Effect of the Organizational Approach in Knowledge Sharing on the Performance of Information Security Management

Edris Abbaszadeh[1], Mohamadreza Sanaei[2*], Reza Ehtesham Rathi[3]

1. Ph.D. Student, Department of IT Management, Qazvin Branch, Islamic Azad University, Qazvin, Iran.
2. Assistant Professor, Department of IT Management, Qazvin Branch, Islamic Azad University, Qazvin, Iran.*(Corresponding Author)*
3. Assistant Professor, Department of Industrial Management, Qazvin Branch, Islamic Azad University, Qazvin, Iran.

Abstract

Introduction: The rapid movement of countries toward the information society has caused the vast growth of information systems and services and the emergence of a new type of organization called virtual organization, which are information-based organizations. Considering the role of information as a valuable commodity in these organizations, the existence of security risks and threats that arise in the virtual environment and through the Internet connection, it is necessary to protect this information and to achieve this The goal of every organization depends on its level of information requires the design of an information security management system so that it can identify and manage the threats that the organization is exposed to and protect its information assets against these attacks and the security of the organization's information. Continuously improving considering the importance of the role of current information in every organization, it seems vital to use information security management systems to set up, implement, control, check, maintain and improve information security.

Method: This study filled the gap in previous writings by considering organizational methods in the study of information security management. A framework was developed based on the framework proposed in the recent work of Perez Gonzalez et al. This framework examined three organizational factors: information security knowledge sharing, observability, and science. In this study, Gonzalez's framework was modified to include two additional organizational factors: commitment and information security learning.

Results: This study identifies the need for managers and decision-makers to consider the role of employees in information security. Managers can influence the levels of motivation, loyalty, and innovative risk-taking of their employees to create an ethical relationship in the organization.

Discussion: This study investigated and analyzed the effects of information security organizational measures (information security knowledge sharing, learning, security observability, security training, and commitment in an organization) on the information security management performance of small and medium companies. The findings show that information security knowledge sharing, learning, and security observability have a significant effect on security performance. In addition, this study clarifies the importance of learning information security and recording acquired knowledge in the commitment of an organization. Regarding information security knowledge sharing, information security learning, and security observability, the results show their positive effect on the information security performance of small and medium companies.

Keywords: Information security, security function; knowledge sharing; Education.

فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

تأثیر روش برخورد سازمانی در اشتراک دانش بر کارکرد مدیریت امنیت اطلاعات

تاریخ دریافت: ۱۴۰۱/۱۲/۲۴
تاریخ پذیرش: ۱۴۰۱/۰۲/۰۸
سال سوم، بهار ۱۴۰۱
شماره اول، صص: ۲۵ - ۳۵

ادریس عباس‌زاده[۱]، محمدرضا ثنایی[۲*]، رضا احتشام‌راثی[۳]

۱.دانشجوی دکتری، گروه مدیریت فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران.Edris_abbaszadeh@yahoo.com
۲.استادیار، گروه مدیریت فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران.mohamadrezasanaei@gmail.com
۳.استادیار، گروه مدیریت صنعتی، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران.MRSEN80@gmail.com

چکیده: وابستگی سازمان‌ها به سیستم‌های اطلاعاتی و سرویس‌های مبتنی‌بر آن (در راستای انجام فعالیت‌ها) از یک‌سو و گستردگی شبکه ایجادشده جهت بهره‌برداری از این سیستم‌ها از سوی دیگر، موجب افزایش میزان آسیب‌پذیری در برابر حوادث امنیتی شده‌است. در این راستا مطالعات محدودی با استفاده از شرکت‌های کوچک و متوسط در بخش تولیدی انجام شده‌است. علاوه بر این، پارامترهای کمی در مطالعات قبلی استفاده‌شده‌اند. این تحقیق با هدف آنالیز تأثیر روش برخورد سازمانی بر کارکرد مدیریت امنیت اطلاعات با به‌کارگیری تعداد زیادی از پارامترها انجام شده است. به همین منظور، یک مدل همراه با فرضیه‌ها برای ارزیابی تأثیر روش برخورد سازمانی بر کارکرد مدیریت امنیت اطلاعات ایجاد شده‌است. داده‌ها از ۱۵۱ کارمند در شرکت‌های کوچک و متوسط تولیدی که از قبل سیاست‌های امنیتی را پیاده‌سازی کرده‌بودند، جمع‌آوری شده‌است. برای ارزیابی نتایج از مدل معادلات ساختاری از طریق نرم‌افزار Amos 22 استفاده‌شده‌است. نتایج ما حاکی از آن است که علم امنیت اطلاعات، مشاهده‌پذیری، اشتراک دانش به‌طور معناداری بر کارکرد امنیت اطلاعات تأثیرمی‌گذارد. به‌علاوه ، این مطالعه تأثیر معنادار آموختن امنیت و ثبت دانش اکتسابی بر تعهد در سازمان را نیز برجسته‌می‌کند.

واژه‌های کلیدی: امنیت اطلاعات کارکرد امنیتی؛ اشتراک دانش؛ آموزش.

۱. مقدمه

حرکت سریع کشورها به‌سوی جامعهٔ اطلاعاتی موجب رشد وسیع سیستم‌ها و سرویس‌های اطلاعاتی و به‌وجودآمدن نوع جدید از سازمان‌ها با عنوان سازمان مجازی شده‌است که سازمان‌هایی مبتنی‌بر اطلاعات هستند. باتوجه به نقش اطلاعات به‌عنوان کالای با ارزش در این سازمان-ها وجود خطرات و تهدیدات امنیتی که درمحیط مجازی و به‌واسطهٔ اتصال به اینترنت به‌وجودمی‌آیند، لزوم حفاظت از این اطلاعات ضروری است و برای دستیابی به این هدف هر سازمان بسته به سطح اطلاعات خود نیازمند طراحی سیستم مدیریت امنیت اطلاعات است تا از این طریق بتواند تهدیداتی که سازمان درمعرض آن قراردارد، شناسایی و مدیریت‌کرده و از سرمایه‌های اطلاعاتی خود در برابر این تجاوزات حفاظت‌کند و امنیت اطلاعات سازمان را پیوسته بهبودبخشد. باتوجه به اهمیت نقش اطلاعات جاری در هر سازمان به‌کارگیری سیستم مدیریت امنیت اطلاعات جهت راه‌اندازی، اجرا، کنترل، چک‌کردن، نگهداری و بهبود امنیت اطلاعات امری حیاتی به‌نظرمی‌رسد؛ از این رو سازمان‌ها و شرکت‌ها ناگزیر به‌دنبال پیاده‌سازی امنیت هستند و این سیستم باید برمبنای نیازهای سازمان و اهمیت اطلاعات طراحی‌شود و می‌تواند پشتیبانی برای فراهم‌کردن سرمایه اطلاعاتی باشد[۱]. با این حال، مشاهده‌شده‌است که مشکلات و راه‌حل‌ها ممکن است به حوزه صنعت بستگی‌داشته‌باشد، زیرا مسائل شرکت‌های کوچک و متوسط تولیدی کاملاً با سایر شرکت‌ها در حوزه‌های دیگر فعالیتی، متفاوت است. امنیت اطلاعات به‌دلیل ماهیت میان‌رشته‌ای آن ،موضوع پیچیده ای است [۲-۶-۸-۹-۲۱]. با توجه به مطالعه فونسکا هررا و همکاران [۹]، رویکرد جامع‌تری برای مدیریت امنیت اطلاعات مورد نیاز است. سیپونن و همکاران [۱۰] پیشنهادکرد که مسائل امنیت اطلاعات باید از منظر مدیریت بررسی شوند.

۲. مبانی نظری پژوهش

مقالات مرتبط به امنیت اطلاعات در شرکت‌ها، عمدتاً بر مسائل مربوط به فناوری تمرکزکرده‌اند و توجه محدودی به استراتژی‌های مدیریتی، استانداردهای امنیتی و خط‌مشی‌ها دارند.

تحقیقات اخیر [۶-۱۰-۲۰] نشان‌می‌دهد که برای درک مدیریت امنیت اطلاعات، به رویکرد جامع‌تری نیاز است. مطالعات پیشین عمدتاً بر عوامل سازمانی و انسانی تمرکزکرده‌اند. با مرور مقالات، درمی‌یابیم که امنیت اطلاعات، مفهوم نسبتاً جدیدی در حوزه مدیریت کسب‌وکار است [۶-۱۰]. با توجه به استفاده عمومی فناوری در کسب‌وکار و امکاناتی که فناوری‌های مبتنی‌بر وب در اختیار قرارمی‌دهند، تأثیر امنیت اطلاعات در تمام فرآیندهای سازمانی افزایش‌یافته‌است.

براساس مقاله پرز-گونزالس و همکاران [۵]، تعداد کمی از مطالعات فقط عوامل سازمانی و انسانی را درنظرگرفته‌اند اما این مطالعات غالباً دریافت کارکنان از امنیت در سازمان‌ها را مورد سنجش [۵-۹-۱۰-۱۴]، که در آن‌ها به‌جای تفکر درباره عوامل معتبر، بررسی مسائل مربوط به سازگاری با اصول امنیت اطلاعات، ایجاد مدل‌ها و چارچوب‌های امنیت داده‌های مدیران اجرایی و بررسی تأیید آن، فقط بر سازمان تأکیدمی-شود. تعداد مقالات نشان‌می‌دهد که بررسی الگوی تحقیق درباره نقش مدیریت در امنیت اطلاعات، امری چالش‌برانگیز است. در این روش، کار سلسله‌مراتبی در امنیت داده‌ها به‌تدریج مهم‌می‌شود و توجه دانشمندان را به خود جلب‌می‌کند.

این بررسی تلاشی برای پرکردن خلاء نوشتارهای قبلی با تمرکز بر روش‌های معتبر است. بنابراین، نقش فرآیندهای مدیریتی در برآورده-کردن آن الزامات از اهمیت ویژه‌ای برخوردار است. این مطالعه خلاء موجود در تحقیقات پیشین را پرمی‌کند. مطالعات گذشته بر جنبه‌های فنی امنیت اطلاعات تمرکزکرده‌اند، درحالی‌که این مطالعه اهمیت فرآیندهای سازمانی و نقش کارکنان را برجسته‌می‌کند.

این مطالعه شامل نوآوری‌های زیر است:

- مدلی برای بررسی تأثیر روش برخورد سازمانی بر کارکرد مدیریت امنیت اطلاعات، توسعه‌داده‌است.
- مطالعات پیشین تنها بر جنبه‌های اندکی از امنیت اطلاعات تمرکزکرده‌اند، اما این مطالعه اهمیت روش‌های سازمانی و نقش کارکنان را نیز برجسته‌کرده‌است.
- این مطالعه نشان‌می‌دهد که کارکنان اغلب به‌صورت غیرعمدی باعث انتشار اطلاعات[1] هستند و آموزش آن‌ها درباره امنیت اطلاعات باید در اولویت باشد.

۳. پیشینه پژوهش

در جستجوی مقالات از ترکیب‌های مختلفی مانند امنیت اطلاعات، پایش کارکرد و پایش کارکرد امنیت اطلاعات استفاده‌شد. چهار مرجع در کار استفاده‌شد: IEEE Xplore، Wiley، World Scientific و ScienceDirect. در نهایت ۳۲ مقاله انتخاب‌شدند تا از داده‌هایشان استفاده‌شود.

[۱] یک چارچوب مبتنی‌بر ISM را برای تصمیم‌گیری مفهوم‌سازی-شده[2] توسعه‌دادند. چارچوب آن‌ها مبتنی‌بر چهار اصل مربوط به کسب-وکار، شامل محیط سازمان، اهداف امنیت اطلاعات، الزامات امنیت اطلاعات و ارزیابی پروتکل‌های امنیت اطلاعات بود. نتایج نشان‌داد که چندین شرکت یا آمادگی کمتری دارند و یا اصلاً آماده نیستند چارچوب پیشنهادی را کاهش‌دهند.

فلورس و همکاران [۱۳] تأثیر ایجاد عوامل حاکمیتی امنیت اطلاعات، که بر اساس فرهنگ به رسمیت شناخته‌شده‌اند، را بررسی-کردند. داده‌های کیفی مطالعه آن‌ها از ۵۷۸ مسئول امنیت اطلاعات در ایالات متحده و سوئد جمع‌آوری‌شد. آن‌ها مشاهده‌کردند که ساختار سازمان، خط‌مشی‌های سازمان و محیط کار مستقیماً بر مدیریت امنیت اطلاعات مبتنی‌بر کسب‌وکار تأثیرمی‌گذارد. همچنین مطالعه آن‌ها مشخص‌کرد که کسب‌وکار باید بر ساختار و مدیریت وظیفه امنیت اطلاعات، تأثیربگذارد.

پارسونز و همکاران [۱۴] یک پرسشنامه براساس جنبه‌های انسانی تهیه‌کردند تا آسیب‌پذیری‌های امنیت اطلاعات ناشی از عامل انسانی را اندازه‌گیری‌کنند. داده‌های ۵۰۰ مدیر اجرایی استرالیایی جمع‌آوری‌شد تا فرضیه پیشنهادی آزمایش‌شود. در این آزمایش قابلیت اطمینان و اعتبار ارزیابی‌شد. نتایج نشان‌داد که کمپین‌های آموزشی تأثیر مثبتی بر آگاهی کارکنان درباره خط‌مشی‌ها و رویه‌ها داشته‌است.

سینگ و گوپتا [۱۵] یک روش ترکیبی را توسعه‌دادند تا عوامل مربوط به مدیریت امنیت اطلاعات را تعیین‌کنند. آن‌ها به‌منظور تجزیه و تحلیل عامل اکتشافی، از تجزیه و تحلیل کلیدواژه‌ها برای داده-های کیفی و از آمارگیری برای داده‌های کمی استفاده‌کردند. نتایج نشان‌داد که عوامل عملیاتی[3]، راهبردی[4] و تدبیری[5] بر مسائل مدیریت امنیت اطلاعات تأثیرمی‌گذارند.

صفا و سولمز[۶]چندین روش رفتار انسانی را ادغام‌کردند تا توسعه اشتراک‌گذاری دانش امنیت اطلاعات در سازمان‌های مختلف را بررسی-کنند. چارچوب مفهومی آن‌ها عوامل مختلفی مانند رفتار[6]، نگرش[7] و مقصود[8] را پوشش‌می‌دهد. یافته اصلی مطالعه آن‌ها این است که عوامل انگیزشی با اشتراک‌گذاری دانش امنیت اطلاعات، همبستگی مثبتی دارد (بر هم تأثیر متقابل مثبت دارند).

سومرو و همکاران [۶] مقالات را به‌صورت سیستمی مرورکردند تا نقش مدیریت در امنیت اطلاعات برای بهبود بهره‌وری را بررسی‌کنند. آن‌ها نتیجه‌گرفتند که مدیریت منابع انسانی، خط‌مشی‌های وابسته به امنیت اطلاعات، زیرساخت شرکت و معماری شرکت تأثیر به‌سزایی در مدیریت امنیت اطلاعات دارند و خاطرنشان‌کردند که اگر مدیران از رویکرد جامع‌تری استفاده‌کنند، می‌توانند نقش مؤثری در مدیریت امنیت اطلاعات ایفاکنند.

هوانگ و همکاران [۷-۲۱] رابطه بین عوامل امنیت سازمانی و دلایل سرپیچی افراد را بررسی‌کردند. داده‌های ۴۱۵ مدیر اجرایی امنیت اطلاعات اسپانیایی جمع‌آوری‌شد، تا فرضیه آن‌ها را ثابت‌کند. نتایج نشان‌داد که نگرانی مدیران امنیت و رفتار همتایان، از دلایل سرپیچی کارکنان است. همچنین مشاهده‌شد که سیستم‌های امنیتی، تحصیلات امنیتی و مشاهده‌پذیری امنیت[9] می‌توانند اطاعت کارکنان را افزایش-دهند.

چوی و همکاران[۱۹] ارتباط بین امنیت اطلاعات و کارکنان درون-سازمانی[10] را بررسی‌کردند. داده‌های کیفی از کارکنان بخش تحقیق و توسعه شرکت‌های چندملیتی جمع‌آوری‌شد. نتایج نشان‌داد که برای تهدیدهای امنیت اطلاعات، باید روش‌های امنیت اطلاعات توسعه‌داده-شوند.

مودی و همکاران [۲۰] یازده نظریه مربوط به دیدگاه رفتاری امنیت سیستم اطلاعات را با هم مقایسه‌کردند. [۲]، در پژوهشی با عنوان ،شناسایی و اولویت‌بندی عوامل انسانی مؤثر بر امنیت اطلاعات با استفاده از رویکرد ترکیبی ANP و DEMATEL فازی بیان‌کردند که امروزه امنیت اطلاعات مسئله‌ای حیاتی بوده و موفقیت سازمان‌ها در سراسر دنیا به آن وابسته است. امنیت سیستم‌های اطلاعاتی هم فناوری و هم افراد (عوامل انسانی) را دربرمی‌گیرد. بر اساس نتایج آنان، پنج شاخص اصلی عبارتند از: ۱-اشاعه استفاده از اطلاعات محرمانه (امنیتی) ۲- سوء استفاده از سیستم اطلاعات (سوءاستفاده عمدی کارمندان داخلی از منابع IS) ۳-آگاهی از اهمیت ضرورت پیروی از قوانین و اجرای فعالیت امنیتی ۴-استفاده از ابزارهای آموزشی متنوع برای آموزش فعالیت‌های مرتبط با امنیت سیستم‌های اطلاعاتی ۵- تعهد و وفاداری کارمندان به سازمان و حفظ اطلاعات .

[۳۱] در تحقیقی با عنوان بررسی ارتباط سیستم‌های سازمان و آگاهی از امنیت اطلاعات دریافتند که ارتباط معناداری بین آگاهی کاربران از امنیت اطلاعات و ابعاد ساختار سازمان رسمی، ابعاد فرهنگ سازمانی و روش‌ها و سیاست‌های منابع انسانی وجوددارد.

جدول ۱. مطالعات مربوطه در زمینه مدیریت امنیت اطلاعات

محدودیت‌ها	هدف	مراجع
مشاهده‌شد که پیاده‌سازی سیستم مدیریت امنیت اطلاعات روی متغیرهای محرمانگی، یکپارچگی، دسترس‌پذیری اثر دارد ولی توضیح داده‌نشده که خط‌مشی امنیت اطلاعات چگونه پیاده‌سازی‌می‌شود و چه پارامترهای برای دستیابی به امنیت اطلاعات وجوددارد.	بررسی و شناسایی عوامل موفقیت استقرار سیستم مدیریت امنیت اطلاعاتISMSدر ایران	[۱]
برای دستیابی به اشتراک-گذاری دانش امنیت اطلاعات در سازمان‌ها، فقط عوامل رفتاری و فرهنگی درنظرگرفته شده اند.	این مطالعه تأثیر ایجاد عوامل حاکمیتی امنیت اطلاعات، که بر اساس فرهنگ به رسمیت شناخته-شده‌اند، را بررسی-کرد.	[۱۳]
باید تأثیر عوامل مداخله ای، فردی و سازمانی بر مدیریت امنیت اطلاعات، نیز مشخص شود.	یک پرسشنامه براساس جنبه‌های انسانی تهیه‌کردند تا آسیب‌پذیری‌های امنیت اطلاعات مبتنی‌بر انسان را اندازه‌گیری‌کند.	[۱۴]
تعداد کمی از عوامل مربوط به مدیریت امنیت اطلاعات درنظر گرفته‌شده‌اند.	یک روش ترکیبی را توسعه‌دادند تا عوامل مربوط به مدیریت امنیت اطلاعات را تعیین‌کنند.	[۱۵]
اندازه نمونه کوچک است و از روش های محدودی	چندین روش رفتار انسانی را ادغام-کردند، تا توسعه	[۶]

برای جمع آوری داده‌ها استفاده‌شده‌است.	اشتراک‌گذاری دانش امنیت اطلاعات در سازمان‌های مختلف را بررسی‌کنند.	
از تعداد محدودی مقاله برای نظرسنجی استفاده-شده‌است و اشاره‌ای به دیدگاه مدیریت نشده‌است.	مقالات را به‌صورت سیستمی مرورکردند، تا نقش مدیریت در مدیریت امنیت اطلاعات برای بهبود بهره‌وری را بررسی‌کنند.	[۱۸]
فقط دو عامل سرپیچی تعیین شدند. رفتارهای واقعی کارکنان در زمینه امنیت اطلاعات، باید اضافه‌شود.	ارتباط بین عوامل امنیت سازمانی و دلایل سرپیچی افراد را بررسی‌کردند.	[۲۱]
باید تأثیر رفتار شهروندی سازمانی به تفصیل ارزیابی-شود.	ارتباط بین امنیت اطلاعات و کارکنان درون‌سازمانی را بررسی کردند.	[۱۹]
مدل پیشنهادی به‌صورت عملی و تجربی اثبات نشده است.	یازده نظریه مربوط به دیدگاه رفتاری امنیت سیستم اطلاعات را با هم مقایسه‌کردند.	[۲۰]
نمی‌توان نتایج را به کل جهان تعمیم‌داد، زیرا داده-های استفاده شده فقط از اسپانیا جمع‌آوری-شده‌اند و توسعه اقتصادی و تکنولوژیکی در کل جهان برابر نیست.	تأثیر روش‌های امنیت سازمانی بر عملکرد مدیریت امنیت اطلاعات را بررسی‌کردند.	[۵]
در این تحقیق، عوامل انسانی (سطح مدیریت) در مدیریت امنیت اطلاعات وجودندارد.	تهدیدهای سازمانی اصلی را از نظر فرآیندهای مدیریت اطلاعات، طبقه‌بندی کردند.	[۳]
تهدیدهای مربوط به افراد مدیر، به‌خوبی درنظرگرفته‌نشده‌است.	چارچوبی برای مدیریت امنیت اطلاعات پیشنهاد-کردند، تا از داده‌ها در برابر بیگانه‌ها، هکرها و افراد غیرمجاز محافظت شود.	[۳۲]
بر اساس نتایج آنان، پنج شاخص اصلی به‌دست‌آمده ولی جامع نیست.	شناسایی و اولویت-بندی عوامل انسانی مؤثر بر امنیت اطلاعات با استفاده از رویکرد ترکیبی ANP و DEMATEL فازی	(زنجیرچی و همکارانش،۱۳۹۳)
باید انواع ساختار سازمانی و نوع روابط افراد در سازمان‌های غیررسمی بررسی‌شود.	بررسی ارتباط سیستم‌های سازمان و آگاهی از امنیت اطلاعات	(Tintamusik,2010)

۴. روش تحقیق

این مطالعه با در ظرگرفتن روش‌های سازمانی در مطالعه مدیریت امنیت اطلاعات، خلاء موجود در نوشتارهای قبلی را پرکرد. یک چارچوب براساس چارچوب پیشنهادی در کار اخیر پرز گونزالز و همکاران (Pérez-González,2019)، توسعه‌داده‌شد. این چارچوب سه عامل سازمانی را بررسی‌می‌کرد: اشتراک‌گذاری دانش امنیت اطلاعات، مشاهده‌پذیری و علم . در این مطالعه چارچوب گونزالز طوری اصلاح‌شد که شامل دو عامل سازمانی اضافی شود: تعهد و آموختن امنیت اطلاعات. شکل ۲ چارچوب مفهومی را نشان‌می‌دهد.

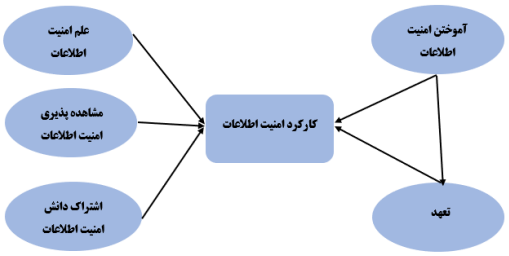
برای دستیابی به اهداف این مطالعه، شش فرضیه براساس ارتباط بین‌سازه‌های[11] چارچوب مفهومی بسط‌داده‌شد. در آزمون فرضیه، مفروضات / فرضیه‌های خود درباره یک نمونه تصادفی ($x = (x_1, \ldots, x_n)$) را آزمایش‌کردیم. فرض می‌تواند این‌گونه باشد که مشاهدات نمونه از یک توزیع نرمال به‌دست‌می‌آیند که توزیع دارای مقدار میانگین معینی است و غیره. فرضی که می‌خواهیم آزمایش‌کنیم معروف به آزمون فرضیه یا فرضیه صفر[12] H_0 است. چند آماره آزمون[13] کاملاً مشخص برای استفاده در انواع مختلف آزمایش‌ها وجوددارد. روش مقدار-p برای بررسی اهمیت آزمایش استفاده‌شده‌است. مقدار-p، ناحیه توزیع صفر در بالای مقدار مشاهده‌شده در آماره آزمون، t_{obs}، است و به‌صورت زیر تعریف-شده‌است:

$$P = P(T \geq t_{obs})$$

اگر مقدار-p از سطح اهمیت کوچک تر باشد، α، فرضیه ردمی‌شود.

با فراگیر شدن و افزایش اهمیت داده‌ها و اطلاعات کمی در جوامع معاصر، آمار نیز به‌عنوان ابزاری برای استخراج دانش از این اطلاعات اهمیت پیدامی‌کند. به‌علاوه، انتظارمی‌رود افرادی که در تجزیه و تحلیل داده‌ها دخالت‌ندارند، اطلاعات آماری را در مورد موضوعاتی مانند انتخابات سیاسی، ویژگی‌های اقتصادی و غیره درک‌کنند و حتی آن را به‌طور انتقادی ارزیابی‌کنند [۲۲-۲۳-۲۴-۳۰] .

در مجموع ۲۰ شرکت کوچک و متوسط شناسایی‌شدند و یک پرسشنامه آنلاین به‌همراه ایمیل‌های پیگیری برای شرکت‌کنندگان ارسال‌شد. این پرسشنامه شامل شش بخش بود: علم امنیت اطلاعات، مشاهده‌پذیری امنیت اطلاعات، اشتراک دانش امنیت اطلاعات، آموختن امنیت اطلاعات، تعهد به یک سازمان و کارکرد مدیریت امنیت اطلاعات. به‌طورکلی، ما ۲۴۰ پرسشنامه ارسال‌کردیم، اما تنها ۱۸۳ پرسشنامه دریافت‌کردیم. از این تعداد، ۱۵۱ پرسشنامه کامل‌بود و برای تجزیه و تحلیل داده‌ها استفاده‌شد.



شکل ۲: چارچوب مفهومی

۱،۴. اشتراک دانش امنیت اطلاعات

اشتراک دانش امنیت اطلاعات، هزینه‌های توسعه ابزارهای حفاظتی جدید را کاهش‌می‌دهد و با افزودن به دانش تهدیدات بالقوه، کارایی ابزارهای فعلی را افزایش‌می‌دهد[۱۹-۱۶-۵] .مطالعات مشترک طیف وسیعی از نقض‌های امنیتی را پوشش‌داده‌است که به نفع همه شرکت‌ها است. بنابراین این بحث به فرضیه زیر منجرمی‌شود:

فرضیه ۱ (H1). اشتراک دانش امنیت اطلاعات با عملکرد امنیت اطلاعات همبستگی مثبت دارد.

۲،۴. علم امنیت اطلاعات

علم امنیت اطلاعات حاصل این مطالعات می‌باشد. پرسنلی با سطح کافی از دانش امنیت اطلاعات به امنیت شرکت می‌افزایند. ضمناً کارکنانی که فاقد این آموزش هستند، شانس بالایی برای تبدیل‌شدن به منبع نقض داده‌ها دارند[۲۷-۳۳] . بر اساس این بحث، فرضیه زیر مطرح‌می‌شود:

فرضیه۲ (H2). علم امنیت اطلاعات با کارکرد امنیت اطلاعات همبستگی مثبت دارد.

۳،۴. مشاهده‌پذیری امنیت اطلاعات

مشاهده‌پذیری امنیت اطلاعات می‌تواند در شرکتی با فرهنگ سازمانی ضعیف و جایی که فشار همتایان ناسازگار زیاد است، موضوع مهمی باشد [۷-۲۰-۲۱] . بنابراین، کارکنان نیازمند کسب آموزش امنیت اطلاعات می‌باشند[۳-۲۰] . هنگام توسعه سیستم‌ها و پروتکل‌های امنیت اطلاعات، شرکت‌ها باید به سه عامل به‌هم‌پیوسته (ثبت دانش اکتسابی امنیت اطلاعات، تجربیات و پایش‌پذیری) مراجعه‌کنند. بنابراین، فرضیه زیر پیشنهادمی‌شود:

فرضیه ۳ (H3). مشاهده‌پذیری امنیت اطلاعات با کارکرد امنیت اطلاعات همبستگی مثبت دارد.

۴،۴. آموختن امنیت اطلاعات

مطالعات اخیر نشان‌می‌دهند که آموزش کارکنان باید خاص و به‌راحتی قابل‌دسترس باشد و جهت بررسی حفظ دانش پیگیری‌شود [۵،۱۳،۱۵،۲۰،۲۷]. مطالعات پیکاری و همکاران [۲۸] نشان‌می‌دهد که آموزش می‌تواند دانش و آگاهی کارکنان در زمینه تهدیدات و عواقب نقض امنیتی را افزایش‌داده و منجر به پیشگیری از چنین حوادثی شود. بااین‌حال،[۱۷] بیان‌می‌کنند که «سازمان‌ها معمولاً کارکنان آموزش‌دیده امنیتی را استخدام‌نمی‌کنند و این امر منجر به آسیب‌پذیری در امنیت اطلاعات آن‌ها می‌شود» . بنابراین، فرضیه‌های زیر مطرح‌می‌شود:

فرضیه ۴ (H4). آموختن کارکنان با تعهد به یک سازمان همبستگی مثبت دارد.

فرضیه ۵ (H5). آموختن کارکنان بر کارکرد امنیت اطلاعات تأثیر مثبت می‌گذارد.

۵،۴. تعهد

برای افزایش تمایل کارکنان به استفاده از هر سرویس، تعهد افراد به عدم افشای سرمایه‌های اطلاعاتی که در دسترس آن‌ها است یک نیاز حیاتی محسوب‌می‌شود این تعهد مکتوب نبوده و به‌صورت رفتار اخلاق‌مدار یا تعهد اخلاقی بیان‌می‌گردد [۲۷-۳۳] .در زمینه امنیت اطلاعات، بسیاری از مطالعات براین باورند که تعهد اخلاقی کارکنان یک سازمان تأثیر قابل‌توجهی بر عملکرد کارکنان در زمینه امنیت اطلاعات دارد[۲۸-۳]. طبق گفته پیکاری و همکاران [۱۷]، بین تعهد کارکنان و کارکرد امنیت اطلاعات همبستگی قوی وجوددارد. به‌طور مشابه، پرز-گونزالس و همکاران [۵] برای تجزیه و تحلیل نقش تعهد در امنیت اطلاعات، مطالعه تجربی انجام‌دادند. بنابراین، فرضیه زیر مطرح‌می‌شود:

فرضیه ۶ (H6). تعهد کارکنان سازمان با کارکرد کارکنان در زمینه امنیت اطلاعات همبستگی مثبت دارد.

۵. تجزیه و تحلیل یافته‌ها

تجزیه و تحلیل داده‌ها شامل یک فرآیند کدگذاری است و برای استخراج اشتراکات و مضامین تکراری از مقایسه مداوم داده‌های محقق استفاده-می‌شود که باعث ظهور مفاهیم جدید پس از مرحله استقرایی‌می‌گردد. تجزیه و تحلیل داده‌ها در یک فرآیند پنج‌مرحله‌ای انجام‌شد. از نرم‌افزار SPSS 25 برای انجام تحلیل عاملی و سپس آزمون پایایی برای همسانی درونی آیتم‌های موجود در مؤلفه‌ها استفاده‌شد. به‌محض کسب نتایج رضایت‌بخش، از نرم‌افزار SPSS Amos 22.0 برای تحلیل عاملی تأییدی (CFA) و تأیید یافته‌ها استفاده‌شد. پس از اعتبارسنجی مدل، روایی ساختار و روایی همگرای مدل آزمایش‌شد. در نهایت، مدل معادلات ساختاری (SEM) برای برآورد روابط بین متغیرهای مستقل و وابسته جهت تأیید یا رد فرضیه انجام‌شد.

۱،۵. تحلیل عاملی اکتشافی

این مطالعه از آزمون‌های Kaiser–Meyer–Oklin (KMO)، و بارتلت برای آزمایش تناسب داده‌ها با تحلیل عاملی استفاده‌کرد. مقدار KMO این مطالعه ۰،۹۰۲ بود که بیش از مقدار توصیه‌شده ۰،۷۰ می‌باشد که کافی محسوب‌می‌شود. آزمون کرویت بارتلت به معنی‌داری آماری رسید که نشان‌می‌دهد داده‌ها برای انجام تحلیل عاملی خوب هستند.

۱۸آیتم تحت آنالیز مؤلفه اصلی (PCA) با نرمالیزاسیون کایزر روش چرخش Varimax برای تحلیل عاملی استفاده‌شدند. آیتم‌ها با بار عاملی کمتر از ۰،۵۰ باید حذف‌شوند (Parsons,2014). بااین‌حال، در این مطالعه بار عاملی همه آیتم‌ها بالای ۰/۵۰ بود و ازاین‌رو، هیچ‌یک حذف-نشد. بنابراین، همه ۱۸ مورد پذیرفته‌شدند و PCA نشان‌داد که آن‌ها در شش جزء گروه‌بندی‌می‌شوند. درصد کل واریانس ۸۳،۸۱۸ بود. ابعاد

فردی ابزار پیشنهادی واریانس کل بیش از ۶۰ درصد را توضیح‌می‌دهد که مناسب‌بودن فرآیند را نشان‌می‌دهد. نتایج PCA را می‌توان در جدول ۲ مشاهده‌کرد.

جدول ۲: نتایج استخراج فاکتورها از گویه‌های پرسشنامه

مولفه ۱	بار عاملی	Eigenvalue	واریانس٪
SV۱	۰.۸۷۳	۹.۶۹۵	۵۵.۳۱۲
SV۲	۰.۸۸۷		
SV۳	۰.۸۹۶		
مولفه ۲	بار عاملی	Eigenvalue	واریانس٪
ST۱	۰.۷۸۹	۱.۹۹۸	۷.۸۸۱
ST۲	۰.۸۷۷		
ST۳	۰.۸۵۲		
مولفه ۳	بار عاملی	Eigenvalue	واریانس٪
SE۱	۰.۷۶۵	۱.۵۲۰	۷.۲۲۵
SE۲	۰.۷۵۹		
SE۳	۰.۸۵۲		
مولفه ۴	بار عاملی	Eigenvalue	واریانس٪
KS۱	۰.۷۸۸	۰.۹۲۱	۵.۴۴۴
KS۲	۰.۷۶۱		
KS۳	۰.۷۷۷		
مولفه ۵	بار عاملی	Eigenvalue	واریانس٪
TR۱	۰.۷۷۱	۰.۹۱۸	۵.۱۲۳
TR۲	۰.۷۱۵		
TR۳	۰.۷۸۱		
مولفه ۶	بار عاملی	Eigenvalue	واریانس٪
SP۱	۰.۷۹۶	۰.۸۵۴	۴.۶۲۲
SP۲	۰.۷۲۲		
SP۳	۰.۷۶۶		
مجموع درصد واریانس : ۸۳.۸۱۸			

۲،۵. آزمون پایایی

این مطالعه از آلفای کرونباخ برای ارزیابی پایایی یا سازگاری درونی آیتم‌ها در شش مؤلفه استفاده‌کرد. به هنگام ارائه ارزیابی کلی از پایایی اندازه‌گیری‌ها، ضریب α پایایی از ۰ تا ۱ متغیر است. اگر همه آیتم‌های مقیاس، مستقل از یکدیگر باشند، α = 0 خواهدبود؛ اگر همه آیتم‌ها کوواریانس بالایی داشته‌باشند، α به ۱ نزدیک می‌شود. هرچه نمره بالاتر باشد، مقیاس حاصل قابل‌اعتمادتر است. ۰،۷ ضریب پایایی قابل‌قبولی است. همان‌طورکه در جدول ۳دیده‌می‌شود، داده‌های پرسشنامه قابل‌اعتماد می‌باشند و می‌توان از آن‌ها برای تجزیه و تحلیل بیشتر استفاده‌کرد.

جدول ۳: مقادیر ضریب آلفای کرونباخ

تعداد گویه ها	آلفای کرونباخ	گویه ها	مولفه
۳	۰.۸۲۲	SV۱,SV۲,SV۳	۱
۳	۰.۹۲۱	ST۱,ST۲, ST۳	۲
۳	۰.۹۱۴	SE۱,SE۲,SE۳	۳
۳	۰.۹۲۳	KS۱,KS۲,KS۳	۴
۳	۰.۸۷۵	TR۱,TR۲,TR۳	۵
۳	۰.۹۲۳	SP۱,SP۲,SP۳	۶

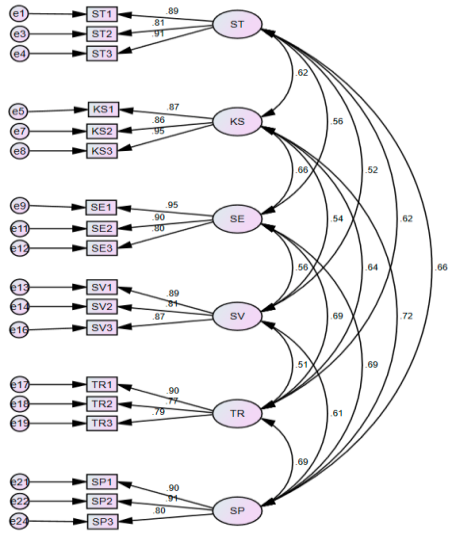
۳،۵. تحلیل عاملی تأییدی

هدف CFA تبیین میزان ارتباط متغیرهای مشاهده‌شده با عوامل پنهان در تحقیق است. CFA روابط بین متغیرها را بر اساس تئوری، تحقیقات تجربی یا هر دو فرض‌می‌کند و سپس ساختار فرضی را به‌صورت آماری آزمایش‌می‌کند. این مدل بر اساس موضوع قبلی این مطالعه ارائه‌شد و از CFA برای تأیید آن استفاده‌گردید. برای انجام CFA از نرم‌افزار SPSS Amos 22 استفاده می‌شود. در مجموع ۱۵۱ همان نمونه مجزا و ۵۱ پارامتر مجزا برآوردشد. درجه آزادی (۵۱-۱۷۱) ۱۲۰ بود و بنابراین مثبت است. بنابراین، مدل شناسایی‌شد و موقعیت مطلوبی برای تجزیه و تحلیل ارائه‌کرد.

همان‌طورکه در شکل ۳ دیده‌می‌شود، مدل اندازه‌گیری نشان‌دهنده الگویی است که در آن هر اندازه‌گیری روی یک عامل خاص بارگذاری‌می‌شود. این مدل نشان‌می‌دهد که چگونه متغیرهای اندازه‌گیری‌شده با هم جمع‌می‌شوند تا ساختار را نشان‌دهند و برای بررسی روایی و پایایی استفاده‌می‌شود. همان‌طورکه در جدول ۴ نشان‌داده‌شد، کوواریانس بین همه متغیرهای پنهان معنی‌دار است زیرا مقدار p کمتر از ۰/۰۵ است.

جدول ۴: کوواریانس بین متغیرهای نهان

			Estimate	SE	CR	P
ST	<->	KS	۰.۶۹۸	۰.۱۵۲	۵.۹۳۵	***
ST	<->	SE	۰.۹۵۸	۰.۱۱۸	۵.۶۸۷	***
ST	<->	SV	۰.۶۸۱	۰.۱۱۵	۵.۳۳۲	***
ST	<->	TR	۰.۷۸۸	۰.۱۳۲	۵.۹۹۸	***
ST	<->	SP	۰.۶۸۹	۰.۱۰۹	۵۶.۵۱۱	***
KS	<->	SE	۰.۷۹۹	۰.۱۵۴	۶.۵۲۳	***
KS	<->	SV	۰.۶۸۷	۰.۱۱۹	۵.۴۵۵	***
KS	<->	TR	۰.۶۸۸	۰.۱۳۹	۶.۴۴۴	***
KS	<->	SP	۰.۷۹۵	.۲۲۲	۶.۴۸۵	***
SE	<->	SV	۰.۷۸۸	۰.۱۳۴	۵.۷۸۴	***
SE	<->	TR	۰.۶۸۷	۰.۱۴۹	۶.۶۸۵	***
SE	<->	SP	۰.۹۸۵	۰.۱۱۸	۶.۸۷۴	***
SV	<->	TR	۰.۷۸۵	۰.۱۲۸	۵.۱۴۵	***
SV	<->	SP	۰.۷۵۸	۰.۱۵۲	۵.۹۸۷	***
TR	<->	SP	۰.۸۸۸	۰.۱۵۴	۶.۸۵۴	***



شکل ۳: مدل اندازه‌گیری

بر اساس SEM با استفاده از SPSS Amos 22، دریافتیم که chi-square (CMIN) = 129.317، درجه آزادی 120=(DF) و سطح احتمال حدود ۰،۰۰۰ بود که ثابت‌کرد این فرضیه معنادار است. CMIN/DF (حداقل اختلاف) ۱،۰۷۸ بود. مقادیر زیر در جدول ۵ در مطالعه ما برای هر پارامتر جهت آزمایش برازش مدل استفاده‌شد.

جدول ۵: اندازه‌گیری مقادیر پارامترهای برازش مدل با SPSS Amos

نام پارامتر	مقدار
شاخص نکوئی برازش	۰،۹۱۴
شاخص برازش تطبیقی	۰،۹۸۸
ریشه میانگین مربعات خطای تخمین (RMSEA)	۰،۰۳۷

جدول ۶: آزمون پایایی ترکیبی

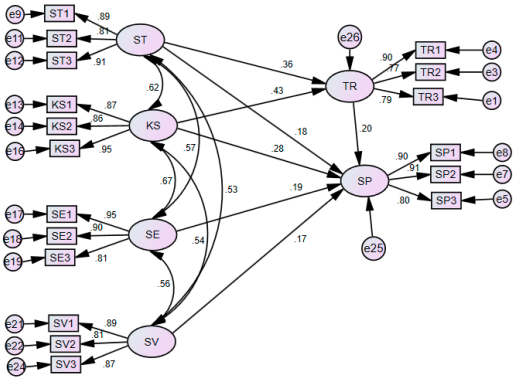
نام پارامتر	مقدار
شاخص نکوئی برازش	۰,۹۲۵
شاخص برازش تطبیقی	۰,۹۹۶
ریشه میانگین مربعات خطای تخمین (RMSEA)	۰,۰۲۲

۴,۵. آزمون روایی و پایایی

جدول ۶، پایایی ترکیبی هر متغیر را نشان‌می‌دهد که در آن تمام متغیرها دارای پایایی ترکیبی بیش از ۰,۷ می‌باشند. درباره روایی در جدول ۶، تمام متغیرها دارای میانگین واریانس بیش از ۰,۵ می‌باشند که پایایی همگرای خوب متغیرها را نشان‌می‌دهد.

۵,۵. تحلیل مسیر مدل معادله ساختاری

در این مطالعه، از نرم‌افزار SPSS Amos 22 برای انجام تحلیل مسیر با استفاده از SEM استفاده‌شد. کل نمونه‌های متمایز ۱۷۱ بود، و تعداد پارامترهای متمایز ۴۹ برآوردشد. درجه آزادی (۱۷۱-۴۹) ۱۲۲ و بنابراین مثبت بود. بنابراین، مدل شناسایی‌شد و وضعیت مطلوبی برای SEM ارائه‌کرد. شکل ۴ نمودار مسیر مدل با استفاده از SPSS Amos را برای تعیین رابطه بین متغیرها نشان‌می‌دهد. بخشی از مدل که نحوه ارتباط متغیرها را مشخص‌می‌کند، مدل ساختاری نامیده‌می‌شود. تخمین‌هایی که بیشترین مقدار را دارند، مهم‌ترین بُعد را در تأثیرگذاری بر متغیرهای وابسته نشان‌می‌دهند.



شکل ۴: نمودار مسیر مدل

جدول ۷: اعتبار افتراقی

	CR Value	AVE
ST	۰.۹۲۳	۰.۷۲۵
KS	۰.۹۵۴	۰.۸۲۲
SE	۰.۹۴۱	۰.۷۲۵
SV	۰.۸۹۹	۰.۷۸۴
TR	۰.۸۲۵	۰.۷۵۴
SP	۰.۹۱۲	۰.۷۹۵

جدول ۸: نتایج استانداردنشده

	ST	KS	SE	SV	TR	SP
ST	۰.۸۵۱					
KS	۰.۶۲۵	۰.۸۵۵				
SE	۰.۵۵۸	۰.۶۵	۰.۸۸۷			
SV	۰.۵۳۶	۰.۵۲۲	۰.۵۹۸	۰.۸۵۵		
TR	۰.۶۲	۰.۶۸	۰.۶۹۲	۰.۵۲۴	۰.۸۵۵	
SP	۰.۶۸۴	۰.۷۲۵	۰.۶۹۸	۰.۶۸۵	۰.۶۹۸	۰.۸۴۵

مقدار p اهمیت تخمین را نشان‌می‌دهد. اگر مقدار p کمتر از ۰,۰۵ باشد، متغیر مستقل بر متغیر وابسته تأثیر معنی‌دار خواهدداشت.

همان‌طورکه در جدول ۸ ارائه‌شده‌است، تمام مقادیر p **** (یعنی ۰,۰۰۰) هستند که کمتر از ۰,۰۵ است. بنابراین، مطالعه حاضر به این نتیجه رسید که همه عوامل - آموزش امنیت، اشتراک دانش، آموزش و مشاهده‌پذیری – به‌طور قابل‌توجهی بر عملکرد امنیتی تأثیر معنی‌دار خواهندداشت. به‌علاوه، این مطالعه تأثیر معنی‌دار آموزش امنیتی و اشتراک دانش بر تعهد به یک سازمان را نشان‌داد.

این مطالعه بر اساس SEM با استفاده از SPSS Amos 22 نشان‌داد که chi-square (CMIN) = 148.862 و درجه آزادی 122 = (DF) می‌باشد. سطح احتمال حدود ۰,۰ ؛ CMIN/DF 1.220 بود. با توجه به Bollen 22، اگر حداقل اختلاف کمتر از ۵ باشد، مدل برازش منطقی است. جدول ۹ مقادیر هر پارامتر را برای آزمایش برازش مدل ارائه‌می‌دهد. مقادیر شاخص بزرگتر از ۰,۹، و مقدار RMSEA کمتر از ۰,۰۵ بود، که نشان ی‌دهد که مدل برازش دارد و مورد تأیید است[۲۹] .

جدول ۹. مقادیر پارامترها برای اندازه‌گیری برازش مدل با SPSS Amos

			Estimate	SE	CR	P
TR	<--	ST	۰.۳۹۸	۰.۰۹۵	۳.۹۵۵	***
TR	<--	KS	۰.۴۵۵	۰.۰۹۵	۴.۶۲۵	***
SP	<--	SV	۰.۱۲۵	۰.۰۶۵	۲.۳۶۲	۰.۰۲۸
SP	<--	SE	۰.۱۴۷	۰.۰۷۵	۳.۵۴۱	۰.۰۲۷
SP	<--	KS	۰.۲۲۵	۰.۰۶۲	۲.۰۵۱	۰.۰۰۴
SP	<--	ST	۰.۱۸۷	۰.۰۵۲	۳.۰۶۵	۰.۰۳۸
SP	<--	TR	۰.۱۸۵	۰.۰۷۱	۲.۲۲۵	۰.۰۲۹

۶. نتیجه‌گیری

در چند سال گذشته، افزایش قابل‌توجهی در نقض امنیت اطلاعات در بخش شرکت‌ها وجودداشته‌است. داده‌های Privacy Rights Clearinghouse نشان‌می‌دهد که از سال ۲۰۰۵، ۷۸۸ مورد نقض داده در شرکت‌های مختلف به‌طور عمومی فاش‌شده‌است که منجر به درخطرافتادن ۱۴,۸ میلیون سند ثبتی شده‌است. ۳۰٪ این نقض‌ها نتیجه خطای انسانی بود[۱۷] .

در حال حاضر، نیاز به تحقیق در مورد اثرات جنبه‌های انسانی برنامه-های امنیت اطلاعات و تأثیر علّی آن‌ها بر سنجش عملکرد امنیت اطلاعات سازمانی وجوددارد. برنامه‌های امنیت اطلاعات که عملکرد کلی امنیت اطلاعات سازمان را افزایش‌می‌دهند، برای کاهش خطای انسانی که منجر به این نوع نقض اطلاعات می‌شود، ضروری هستند. این مطالعه اثرات اقدامات سازمانی امنیت اطلاعات (اشتراک دانش امنیت اطلاعات، آموختن، مشاهده‌پذیری امنیت، آموزش امنیتی و تعهد در یک سازمان) را بر عملکرد مدیریت امنیت اطلاعات شرکت‌های کوچک و متوسط بررسی و تحلیل کرد. یافته‌ها نشان‌می‌دهند اشتراک دانش امنیت اطلاعات، آموختن، مشاهده‌پذیری امنیت، بر عملکرد امنیتی تأثیر معنی-دار دارند. به‌علاوه، این مطالعه اهمیت آموختن امنیت اطلاعات و ثبت دانش اکتسابی در تعهد یک سازمان را روشن‌می‌سازد.

در مورد اشتراک دانش امنیت اطلاعات، آموختن امنیت اطلاعات و مشاهده‌پذیری امنیتی، نتایج، تأثیر مثبت آن‌ها بر کارکرد امنیت اطلاعات شرکت‌های کوچک و متوسط را نشان‌می‌دهند. این یافته‌ها، مؤید تحقیقات اخیر مانند فلورس و همکاران می‌باشند [۷-۲۱] دریافتند که این عوامل ابزارهای موثری در توسعه کارکرد امنیت اطلاعات سازمان‌ها هستند.

با توجه به تعهد افراد در یک سازمان، این مطالعه تأثیر آن بر کارکرد امنیت اطلاعات را تجزیه و تحلیل و بررسی‌کرد. نتایج نشان‌دهنده رابطه مثبت بین این دو ساختار است که یافته‌های تحقیقات جدید، قبلی را تأییدمی‌کند [۲۱] . به‌علاوه، در مورد آموختن امنیت اطلاعات، یافته‌های این مطالعه تأثیر مثبت آموختن امنیت بر تعهد افراد به سازمان و کارکرد امنیت اطلاعات را نشان‌می‌دهد. این نتیجه توسط مطالعاتی مانند [۱۴-۱۹] تأییدمی‌شود. بنابراین، کارکرد امنیت اطلاعات در شرکت‌های کوچک و متوسط صنعتی به‌طور مثبت تحت‌تأثیر ثبت علم امنیت اطلاعات، مشاهده‌پذیری، آموختن، تعلم و تعهد به یک سازمان است. هنگامی که مدیریت امنیت اطلاعات به‌عنوان یک مزاحم یا مانع برای تکمیل کار تلقی‌می‌شود، کارمندان می‌توانند از قوانین امنیتی وخط مشی پیروی‌نکنند. مدیریت می‌تواند این خطر را با آموزش صحیح به کارکنان خود در مورد رایانه‌ها و سیستم‌های داده‌ای که برای تکمیل وظایف کارمی‌کنند، کاهش‌دهد. تحقیقات نشان‌می‌دهد که مهارت‌های کامپیوتری و سطح تجربه می‌تواند بر رفتار امنیتی بالقوه کارمند تأثیربگذارد [۳۰-۲۹] . سازمان‌ها باید سیستم‌های اطلاعاتی کارکنان و آموزش-های امنیتی را ارائه‌دهند که برای ازبین‌بردن خطاها کافی باشند. آموزش باید به روش‌های مختلف ارائه‌شود که شامل مواردی مانند آموزش کلاسی، آموزش آنلاین از طریق ارائه مبتنی‌بر وب و ویدئو، خبرنامه‌ها، پوسترها و آگهی‌ها است. یک سازمان از این تنوع منتفع-می‌شود، زیرا اجازه‌می‌دهد محتوا چندین بار و به روش‌های مختلف ارائه-شود. تحصیلات امنیتی باید به‌طور منظم نظارت و ارزیابی‌شود.

این مطالعه نیاز مدیران و تصمیم‌گیرندگان به درنظرگرفتن نقش کارکنان در امنیت اطلاعات را شناسایی‌می‌کند. مدیران می‌توانند بر سطوح انگیزه، وفاداری و ریسک‌پذیری نوآورانه کارکنان خود برای ایجاد یک رابطه اخلاق‌مدار در سازمان تأثیربگذارند. یک ابزار قوی برای تأثیرگذار بودن یک مدیر، داشتن یک رابطه اخلاق مدار با کارکنان است. چنین ابتکاراتی به‌طور مثبت بر عملکرد مدیریت امنیت اطلاعات و همچنین سودآوری سازمان تأثیرمی‌گذارد. یک مدیر خوب، از طریق اعتماد کارکنان و سازمان، ممکن است به اهداف سازمانی دست‌یابد. آموزش امنیت اطلاعات جنبه دیگری برای بهبود عملکرد سنجش امنیت اطلاعات است که حاصل مطالعه ما می‌باشد.

به‌علاوه، کارگاه های آموزشی برای سازمانی که به‌دنبال مزیت رقابتی از طریق نیروی کار بسیار ماهر و انعطاف‌پذیر است، ضروری می‌باشد. یک استراتژی آموزشی مؤثر، کارکنان را قادرمی‌سازد تا به استفاده از فناوری‌های جدید اطمینان‌داشته‌باشند و تغییراتی را در امنیت اطلاعات ایجادکنند. آموزش مداوم برای بررسی و به‌روزرسانی دانش و مهارت‌های کارکنان مورد نیاز است، زیرا باعث‌می‌شود آن‌ها از نظر عملکردی در عملکرد مدیریت امنیت اطلاعات خود مؤثر واقع‌شوند. سیاستگذاران باید جلسات آموزشی برای کارکنان ترتیب‌دهند تا سنجش امنیت اطلاعات را بهبودبخشند. تأکید بر نقش‌ها و مسئولیت‌های کارکنان، شخصی‌سازی برای انطباق را فراهم‌کرده و مالکیت را ارتقامی‌دهد. شخصی‌سازی به کارمند نقش فعالی در انطباق می‌دهد و مفهوم محدودکننده را کاهش-می‌دهد. خط‌مشی‌ها باید به‌راحتی دردسترس باشند، به‌صورت دوره‌ای بازبینی‌شوند و برای همه اعضا، شرکا و عوامل سازمان اعمال‌شوند. این مسئولیت مدیریت سازمانی است که از فرآیند ساخت خط‌مشی مدیریت امنیت اطلاعات پشتیبانی‌کند. بنابراین، مدیریت باید اطمینان حاصل‌کند که کارکنان به‌طور کامل سیاست‌ها را درک‌کرده و آن‌ها را به‌خوبی درک-می‌کنند. علاوه‌بر این، مدیریت سازمانی باید نقش فعالی در ایجاد انگیزه در کارکنان خود برای رعایت خط‌مشی‌ها ایفاکند. همان‌طورکه در این مطالعه مطرح‌شده‌است، کارمندان اغلب منبع نقض ناخواسته داده‌ها هستند و آموزش آن‌ها در زمینه امنیت اطلاعات باید در اولویت قرارگیرد.

اگر سازمان روابط کاری سالمی را که به مدیران در تسهیل تغییرات سازمانی کمک‌می‌کند، ارتقادهد، یافته‌های مطالعه ما می‌تواند برای افزایش عملکرد سنجش امنیت اطلاعات مفید باشد. کارکنان درصورت اعتماد بیشتر مستعد پذیرش دستورالعمل‌های مدیر خود هستند. این نیز به رهبری اجازه‌می‌دهد تا کارکنان را تشویق‌کند که به اهداف و تغییرات سازمانی متعهدشوند. وجود تعهد اخلاقی در کارمند به‌عنوان یک تعدیل‌کننده مثبت برای کاهش تردید کارمند تلقی‌می‌شود. یافته‌ها محدود به تفسیر این محقق بوده و می‌تواند معنای متفاوتی برای سایر محققین داشته‌باشد. روش علمی جمع‌آوری داده‌ها و تجزیه و تحلیل داده‌ها که توسط روش تحقیق انتخاب‌شده مورد نیاز است، اثبات مفاهیم ازطریق داده‌های به‌دست‌آمده، سوگیری را کاهش‌می‌دهد. اگرچه یافته‌های این مطالعه متشکل از روایت‌های مردان و زنان شاغل در صنایع مختلف بود، اما مشارکت، محدود به متخصصان سازمانی بود که به‌عنوان کارگران دفتری شناخته‌می‌شوند. این کارگران در نقش خود متخصصانی بودند که وظایف اداری و استراتژیک را انجام‌می‌دادند. در مقابل، کارگران مزدبگیر، معروف به کارگران اصلی، کار یدی را انجام‌می‌دهند. از آنجاکه فقط کارگران اداری پرسشنامه را پرکردند، داده‌ها محدود بود. نظرات کارگران اصلی جمع‌آوری‌نشد. تحقیقات بیشتر که شامل کارگران اصلی باشد می‌تواند راه دیگری برای مشاهده اعتماد یا تعیین اینکه آیا می‌توان سطوح یکسانی از اخلاق‌مداری را بین کارگران اصلی و دفتری یک سازمان، ارائه‌کند.

عامل انسانی مهمترین عامل در امنیت اطلاعات است. این به‌دلیل نقش کارمند در نقض داده‌ها و پیروی از خط‌مشی است. هدف این مطالعه بررسی و تحلیل تأثیر رویکردهای سازمانی بر کارکرد امنیت اطلاعات می‌باشد.غالب مطالعات موجود عمدتاً بر جنبه‌های فنی امنیت اطلاعات با توجه محدود به فرآیندهای سازمانی متمرکزند. بنابراین،

هدف ما این بود که با بررسی و تحلیل رابطه بین عوامل سازمانی و عملکرد امنیت اطلاعات، این شکاف تحقیقاتی را برطرف‌کنیم. از نظر مفاهیم کاربردی، یافته‌های این مطالعه پیامدهای مهمی را برای مدیران و سیاست‌گذاران دربارهٔ عوامل سازمانی تقویت‌کنندهٔ عملکرد امنیت اطلاعات کارکنان، ارائه‌می‌کند. بنابراین، باید بر عملکرد امنیت اطلاعات بر اساس اثربخشی آن‌ها در تقویت استعداد و رفتار امنیتی کارکنان تأکیدشود. اندازه‌گیری عملکرد امنیت اطلاعات، نگرش کلی سازمان را نسبت به امنیت اطلاعات و انطباق با آن را نشان‌می‌دهد. بنابراین با هر کنترل امنیتی فنی از نظر سطح برنامه استراتژیک و سطح سرمایه‌گذاری برخورد یکسانی شود.

این تحقیق علی‌رغم محاسن خود، دارای محدودیت‌هایی است. این مطالعه رویه‌های سازمانی و تأثیر آن‌ها بر عملکرد امنیت اطلاعات مطالعه‌کرد. با این‌حال، سایر جنبه‌ها مانند فرهنگ و وفاداری کارکنان نیاز به بررسی دارند. بنابراین، تحقیقات آتی می‌توانند برای درک همه عواملی که بر کارکرد امنیت اطلاعات تأثیرمی‌گذارد، این فاکتورها را نیز درنظربگیرند.

منابع

[۱] نورایی، فرزاد. (۱۳۹۱). بررسی و شناسایی عوامل موفقیت استقرار سیستم مدیریت امنیت اطلاعات ISMS در ایران (مطالعه موردی بانک دی)، (پایان‌نامه کارشناسی‌ارشد). دانشگاه سیستان و بلوچستان، زاهدان.

[۲] زنجیرچی،س.م.، مروتی شریف‌آبادی، ع. و شاه‌حسینی بیده، ش.(۱۳۹۳). مقایسهٔ عملکرد سازمان‌ها در پیاده‌سازی مدیریت ارتباط با مشتری با استفاده از رویکرد ترکیبی NAP و DEMATEL فازی، فصلنامه بازاریابی نوین، ۴(۳)،۲۱۲-۱۹۵.

[3] Kobes, P. Human factor aspects in information security management in the traditional IT and cloud computing models. Oper. Res.Decis. 2021, 1, 61–76.

[4] Florez, H. A Model of an Information Security Management System Based on NTC-ISO/IEC27001 Standard. IAENG Int. J. Comput. Sci. 2021, 48, IJCS_48_2_01

[5] Pérz-González, D.; Prciado, S.T.; Solna-Gonzalez, P. Organizational practices as antecedents of the information security management performance: An empirical investigation. Inf. Technol. People 2019, 32, 1262–1275

[6] Safa, N.S.; Von Salms, R. An information security knowledge sharing model in organizations. Computer. Hum. Behavior. 2016, 57, 442–451

[7] Hwang, I.; Kim, D.; Kim, T.; Kim, S. Why not comply with information security? An empirical approach for the causes of non-compliance. Online Inf. Rev. 2017.

[8] Miladinovi, V.T. Development of Awareness and Competences of Employees in the Processes of Information Security Management System: Guidelines for practical application. JITA-J. Inf. Technol. Appl. 2020, 20, 87–95.

[9] Putra, I.M.M.; Mutijrsa, K. Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005. In Proceedings of the 2021 3rd East Indonesia Conference on Computer and Information Technology (EI Con CIT), Surabaya, Indonesia, 9–11 April 2021; pp. 14–19.

[10] Siponen, M.; Pahnila, S.; Mahmood, M.A. Compliance with information security policies: An empirical investigation. Computer 2010, 43, 64–71.

[11] Marlli, L.; Lievrouw, E.; Van Hoyweghen, I. Fit for purpose? The GDPR and the governance of European digital health. Policy Stud. 2020, 41, 447–467.

[12] Ma, Q.; Schmidt, M.B.; Person, J.N. An Integrated Framework for ISM. 2009, 20, 95–107.

[13] Rocha Flores. Antansn, E Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture. Computer. 2014, 43, 90–110.

[14] Parsons, K.; M. Cormac, Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computer. Security. 2014, 42, 165–176.

[15] Singh, A.N.; Gupt, M.; Ojha, A. Identifying factors of "organizational information security management". J. Enterp. Inf. Manag.2014, 27, 644–667.

[16] Willison, R. Warkentin, M. Beyond deterrence: An expanded view of employee computer abuse. MIS Q. 2013, 37, 1–20

[17] Peikare, T.; Shah, M.H.; Lo, M.C. Patients' perception of the information security management in

[18] Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. Int. IT. Management. 2016, 36, 215–225.

[19] Cho, S.; Martins, J.T.; Bernik, I. Information security: Listening to the perspective of organizational insiders. J. Inf. Sci. 2018, 44,752–767.

[20] Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. MIS Q. 2018, 42,285–311.

[21] Hwang, I.; Cha, O. Examining technostress creators and role stress as potential threats to employees' information security compliance. Computer. Hum. Behavior. 2018, 81, 282–293

[22] Shaukat, K. A review of time-series anomaly detection techniques: A step to future perspectives. Vancouver, BC, Canada, 29–30 April 2021; pp. 865–877.

[23] Shaukat, K.; Luo, S.; Chen, S.; Liu, D. Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. In Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 20–21 October 2020; pp. 1–6.

[24] Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Chen, S.; Liu, D.; Li, J. Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies 2020, 13, 2509.

[25] Mamonov, S.; Benbunan-Fich, R. The impact of information security threat awareness on privacy-protective behaviors. Comput. Hum. Behav. 2018, 83, 32–4.

[26] health centers: The role of organizational and human factors. BMC Med Inform. Decis. Mak. 2018, 18, 102.

[27] Bentler, P.M.; Bonett, D.G. Significance tests and goodness of fit in the analysis of covariance structures. Psychol. Bull. 1980,88, 588.

[28] Bollen, K.A. Structural Equations with latent Variables; John Wiley & Sons: New York, NY, USA, 1989; p. 210. (accessed on 16 September 2021).

[29] Qu, X. Multivariate Data Analysis; Taylor & Francis: London, UK, 2007; (accessed on 16 September 2021).

[30] Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Xu, M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access 2020, 8, 222310–222354.
[31] Tintamusik, Y. (2010). Examining the relationship between organization systems and information security awareness, (Doctoral Dissertation). Business Administration. Northcentral University. Retrieved from https://eric.ed.gov/?id=ED516884
[32] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-220.
[33] Bentler, P.M. Comparative fit indexes in structural models. Psychol. Bull. 1990, 107, 238.

پی‌نوشت

1. Breaches
2. Data conceptualized decision-making
3. Operational
4. Strategic
5. Tactical
6. Behavior
7. Attitude
8. Intention
9. security visibility
10. organizational insiders
11. Constructs
12. null hypothesis
13. test statistic