

Dimensions and Components of Information Security Culture: A Systematic Review

Soheila Jafarnezhad Sany*

PhD Candidate in Information Technology Management; Faculty of Management and Accounting; Allameh Tabataba'i University; Tehran, Iran Email: Jafarnezhad.sany@gmail.com

Mohammadreza Taghva

PhD in Systems Development Management; Professor; Faculty of Management and Accounting; Allameh Tabataba'i University; Tehran, Iran Email: taghva@gmail.com

Mohammad Taghi Taghavifard

PhD in Industrial Engineering; Professor; Faculty of Management and Accounting; Allameh Tabataba'i University; Tehran, Iran; Email: dr.taghavifard@gmail.com

Mirali Seyednaghavi

PhD in Public Management; Professor; Faculty of Management and Accounting; Allameh Tabataba'i University; Tehran; Email: Iran.asnagavi@yahoo.com

Iranian Journal of
**Information
Processing and
Management**

Iranian Research Institute

for Information Science and Technology
(IranDoc)

ISSN 2251-8223

eISSN 2251-8231

Indexed by SCOPUS, ISC, & LISTA

Vol. 38 | No. 4 | pp. ??-??

Summer 2023

<https://doi.org/ijpm.38.4>



Received: 06, Jul. 2022 | Accepted: 07, Nov. 2022

Abstract: Creating an information security culture helps to minimize threats, especially threats caused by humans, in order to protect information, and as a result, it leads to the reduction of data breaches or incidents in organizations. No study has been conducted to identify the components of information security culture in the country so far. Information security culture has been investigated and analyzed using different approaches and based on different theories. The purpose of this article is to review the existing researches in the field of information security culture in order to investigate the knowledge resulted and identify the dimensions and components of the information security culture and integrate the literature in this field.

In order to carry out this systematic review, all the studies conducted in the field of information security culture were extracted from reliable databases using relevant keywords. Finally, 310 related articles from 2000 to 2022 were reviewed. Based on the results of this study and according to the purpose of the research, the components and dimensions of information security culture with different approaches and perspectives were identified and compiled.

The research findings indicate that there is no widely accepted set of

* Corresponding Author

dimensions and components. Different researchers have considered different dimensions and components for the information security culture. They have used 3 theories and concepts in their studies. The frequency of theories used in different researches was determined and the most commonly used one is Schein's organizational culture model. Also the mentioned researches have been carried out in various organizations and industries. There is no industry-specific model or framework provided. Also, most of the proposed models or frameworks are descriptive and have not been evaluated, and in terms of geographical division, the researches were also examined and it was found that most of the researches belong to developing countries.

Keywords: Information Security, Information Security Culture, Organizational Culture, Systematic Review



ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات:

یک مرور نظام‌مند

سهیلا جعفر نژاد ثانی

دانشجوی دکتری مدیریت فناوری اطلاعات؛
دانشکده مدیریت و حسابداری؛
دانشگاه علامه طباطبائی؛ تهران، ایران؛
پدیده‌آور رابط Jafarnezhad.sany@gmail.com

محمد رضا تقوی

دکتری مدیریت توسعه سیستم‌ها؛ استاد؛
دانشکده مدیریت و حسابداری؛ دانشگاه علامه طباطبائی؛
تهران، ایران taghva@gmail.com

محمد تقی تقوی فرد

دکتری مهندسی صنایع؛ استاد؛ دانشکده مدیریت و
حسابداری؛ دانشگاه علامه طباطبائی؛ تهران، ایران؛
dr.taghavifard@gmail.com

میر علی سید تقوی

دکتری مدیریت دولتی؛ استاد؛ دانشکده مدیریت و
حسابداری؛ دانشگاه علامه طباطبائی؛ تهران، ایران؛
asnagavi@yahoo.com



دریافت: ۱۴۰۱/۰۴/۱۵ پذیرش: ۱۴۰۱/۰۸/۱۶ مقاله برای اصلاح به مدت ۴۸ روز نزد پدیدآوران بوده است.

چکیده: ایجاد فرهنگ امنیت اطلاعات در به حداقل رساندن تهدیدات، به ویژه تهدیدات انسانی در جهت حفاظت از اطلاعات کمک می‌کند و در نتیجه، به کاهش نقض داده‌ها یا حوادث در سازمان‌ها منجر می‌شود. تاکنون مطالعه‌ای جهت شناسایی مؤلفه‌های فرهنگ امنیت اطلاعات در کشور صورت نگرفته است. بر اساس نظریه‌های مختلف، فرهنگ امنیت اطلاعات با رویکردهای مختلفی بررسی و مورد تجزیه و تحلیل قرار گرفته است. هدف این مقاله بررسی تحقیقات موجود در حوزه فرهنگ امنیت اطلاعات و شناسایی ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات و یکپارچه‌سازی ادبیات این حوزه است.

به منظور انجام این مرور نظام‌مند کلیه مطالعات انجام گرفته در حوزه فرهنگ امنیت اطلاعات با استفاده از کلیدواژه‌های مرتبط از پایگاه داده‌های معتبر استخراج شد و سرانجام، تعداد ۳۱۰ مقاله مرتبط از سال ۲۰۰۰ تا ۲۰۲۲ مورد بررسی قرار گرفت. بر اساس بررسی صورت گرفته و با توجه به هدف پژوهش، مؤلفه‌ها و ابعاد فرهنگ امنیت اطلاعات با رویکردها و دیدگاه‌های متفاوت شناسایی و گردآوری گردید.

تشریح علمی | رتبه بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران
(ایرانداک)

شاپا (جایی) ۲۲۵۱-۸۲۲۳

شاپا (الکترونیکی) ۲۲۵۱-۸۲۳۱

نمایه در SCOPUS، ISC، LISTA، و

jipm.irandoc.ac.ir

دوره ۳۸ | شماره ۴ | صص ۱۲۵۷-۱۲۸۲

تابستان ۱۴۰۲

<https://doi.org/jipm.38.4>



یافته‌های پژوهش حاکی از آن است که مجموعه‌ای از ابعاد و مؤلفه‌ها که به‌طور گسترده پذیرفته شده باشند، وجود ندارد و محققان مختلف، ابعاد و مؤلفه‌های متفاوتی برای فرهنگ امنیت اطلاعات در نظر گرفته‌اند. محققان از ۳ تئوری و مفهوم در مطالعات خود استفاده نموده‌اند. فراوانی تئوری‌های مورد استفاده در پژوهش‌های مختلف مشخص شد و بیشترین تئوری مورد استفاده، مدل فرهنگ سازمانی «شاین» است. پژوهش‌ها در سازمان‌ها و صنایع مختلفی انجام گرفته، ولی مدل یا چارچوبی مختص به یک صنعت خاص ارائه نشده است. همچنین، بیشتر مدل‌ها یا چارچوب‌های پیشنهادی جنبه توصیفی داشته و مورد ارزیابی قرار نگرفته‌اند. از لحاظ تفکیک جغرافیایی نیز پژوهش‌ها مورد بررسی قرار گرفت و مشخص گردید که بیشترین آن‌ها به کشورهای در حال توسعه تعلق دارند.

کلیدواژه‌ها: امنیت اطلاعات، فرهنگ امنیت اطلاعات، فرهنگ سازمانی، مرور نظام‌مند

۱. مقدمه

سازمان‌ها روزبه‌روز بر اطلاعات و سیستم‌های اطلاعاتی بیشتر تکیه می‌کنند و مبحث امنیت اطلاعات نیز هرچه بیشتر مورد توجه قرار می‌گیرد. نقض امنیت اطلاعات همواره منجر به زیان‌های اقتصادی و نیز موجب اثرات منفی بر شهرت و اعتماد یک سازمان می‌شود. تحقیقات بسیاری در زمینه توسعه ابزارهای فنی جهت ایمن‌سازی و حفاظت از دارایی‌های اطلاعاتی سازمان‌ها صورت گرفته است. با این حال و با توسعه فناوری، این ابزارها کافی نیستند و همچنان نقض در امنیت اطلاعات وجود دارد. محققان و متخصصان امنیت اطلاعات به‌طور فزاینده‌ای تأکید دارند که نمی‌توان از خطرات و تهدیدات امنیتی، صرفاً با ابزارهای فنی اجتناب کرد و عوامل دیگری در سازمان‌ها می‌تواند بر امنیت کل سازمان تأثیر بگذارد. تحقیقات نشان می‌دهد که بسیاری از حوادث و نقض‌های امنیتی به دلیل سهل‌انگاری انسان (عمدی یا غیرعمدی) اتفاق افتاده است. یک مطالعه بر روی رفتار متخصصان امنیتی به این نتیجه رسید که ۴۳ درصد از نقض اطلاعات به دلیل رفتار کارمندان است (Dong et al. 2021). در سال ۲۰۱۴، شاخص اطلاعات امنیت سایبری آی‌بی‌ام تقریباً ۹۵ درصد از حوادث امنیت اطلاعات را شامل سهل‌انگاری کارکنان گزارش کرد (IBM 2014). اقدامات امنیتی فنی در طول سال‌ها مفید بوده‌اند، اما نقض‌های امنیتی و تهدیدها همچنان در حال افزایش است. مهاجمان رفتار کارکنان را برای اجرای فعالیت‌های مخرب خود هدف قرار می‌دهند. یک مطالعه بریتانیایی به این نتیجه رسید که ۵۸ درصد از حملات در سازمان‌های بریتانیایی به دلیل تهدیدات داخلی است (Ali et al. 2021). سازمان‌ها

می‌توانند جدیدترین راه‌حل‌های امنیتی فناوری را پیاده‌سازی کنند، اما کارکنان هنوز افرادی هستند که اغلب ناآگاهانه از طریق رفتارهای خود که ناشی از فرهنگ ضعیف امنیت اطلاعات است، نقض‌های امنیتی به وجود می‌آورند.

با توجه به اینکه فناوری اطلاعات و ارتباطات به عنوان سیستم‌های فنی-اجتماعی در نظر گرفته شده است، سازمان‌ها تنها زمانی می‌توانند ایمن باشند که عناصر فنی و اجتماعی-فرهنگی آن‌ها با هم هماهنگ باشد. توجه و تمرکز بر فرهنگ امنیت اطلاعات^۱ به سال‌ها قبل بازمی‌گردد، ولی توجه به این امر امروزه نیز یک مسئله حیاتی است و دانشگاه و صنعت برای مبارزه با تهدیدات حفاظت از اطلاعات تلاش می‌کنند (Da Veiga et al. 2020). از آنجا که فرهنگ امنیت سهم قابل توجهی در حوزه امنیت اطلاعات دارد، مطالعه فرهنگ امنیت ضروری است. به‌رغم توصیه‌های بسیار محققان برای ایجاد فرهنگ امنیت اطلاعات، فقدان فرهنگ امنیت اطلاعات همچنان وجود دارد، به‌خصوص در جنبه‌هایی که می‌تواند رفتار امنیتی کارمندان را بهبود بخشد (Nasir, Abdullah Arshah & Hamid 2019). ترکیب فناوری و آگاهی انسانی و صلاحیت می‌تواند سطح امنیت کلی یک سازمان را تا حد زیادی بهبود بخشد. هدف از این پژوهش رسیدن به درک بهتری از فرهنگ امنیت اطلاعات و ابعاد آن در سازمان‌هاست. این پژوهش می‌تواند با بازشناسایی مؤلفه‌های تأثیرگذار بر فرهنگ امنیت اطلاعات، به مطالعات بیشتر در ارتباط با فرهنگ امنیت اطلاعات در سازمان‌ها جهت بهبود آگاهی امنیتی و سرانجام، رفتارهای امن‌تر کارکنان کمک نماید.

فرهنگ امنیت اطلاعات به عنوان روشی مؤثر برای ارتقای رفتار ایمن و مدیریت ریسک‌های امنیتی در سازمان پذیرفته شده است. فرهنگ امنیت اقدامات اجتماعی، فرهنگی و اخلاقی جهت بهبود رفتار امنیتی اعضای سازمان را در برمی‌گیرد. این موضوع بر بخش کوچکی از ارزش‌ها و رفتارهای انسانی متمرکز است و همه ارزش‌های اساسی انسانی، هنجارها و باورهای را که فرهنگ سازمانی را تحت تأثیر قرار می‌دهند، پوشش نمی‌دهد. گفته شده است که سنجش امنیت و فرهنگ فرایند پیچیده‌ای است که بررسی آن زمان‌بر است و تعمیم آن به جمعیتی بیشتر، بسیار دشوار است (Schlienger & Tufel 2003). در نتیجه، چالشی که پیش‌روست، کمیت و بررسی عناصر حیاتی است که

1. information security culture (ISC)

فرهنگ امنیتی را مفهوم‌سازی و اندازه‌گیری می‌کند. برخی ادبیات موجود الگوی فرهنگ سازمانی «شاین»^۱ را جهت مطالعه فرهنگ امنیت اطلاعات اتخاذ کرده‌اند. این مطالعات نشان داد که همه عناصر و موضوعات امنیت اطلاعات را می‌توان در سه سطح مدل فرهنگ سازمانها (مصنوعات^۲، ارزش‌ها و مفروضات) بیان نمود. این مطالعات نشان می‌دهند که فرهنگ امنیت اطلاعات محصولی از عوامل مختلف است که بر رفتار افراد بر اساس محیط سازمان تأثیر می‌گذارد. «چان» و همکاران اظهار داشته‌اند که یکی از دلایل اصلی نگرانی‌ها و چالش‌هایی که در سازمان ایجاد می‌شود آن است که کارکنان در رعایت خط‌مشی‌ها و دستورالعمل‌های امنیت اطلاعات بسیار کوتاهی می‌کنند (Chan, Woon & Kankanhalli 2005). تأکید بر این نکته مهم است که حفظ امنیت اطلاعات یک سازمان نه تنها مسئولیت و وظیفه متخصصان فناوری اطلاعات در داخل سازمان است، بلکه وظیفه و مسئولیت همه کارکنان و افرادی است که در محیط سازمان هستند (Rotvold 2008).

به نظر می‌رسد که همراه با افزایش علاقه به فرهنگ امنیت اطلاعات، در مورد اینکه فرهنگ امنیت اطلاعات در واقع چیست، تردید و توافق کمی وجود دارد. بنابراین، تعریف‌ها و دیدگاه‌های چندی در مورد این موضوع وجود دارد. در زیر به برخی از تعاریف فرهنگ امنیت اطلاعات اشاره می‌گردد:

«ون سولمز» خواستار ایجاد فرهنگ امنیت اطلاعات در سازمانها، «با القای جنبه‌های امنیت اطلاعات به هر کارمند به‌عنوان یک روش طبیعی برای انجام شغل روزمره» است (Von Solms 2000). «مارتینز و ایلوف» آن را محصول رفتار مرتبط با امنیت اطلاعات کارمندان توصیف می‌کنند که با گذشت زمان به «روش‌های انجام کار» تبدیل می‌شود (Martins & Ellif 2002). «شلینگر و تیوفل» فرهنگ امنیت اطلاعات را به‌عنوان کلیه اقدامات فرهنگی اجتماعی که از روش‌های فعالیت فنی پشتیبانی می‌کنند، تعریف کردند. به‌طوری که امنیت اطلاعات به یک جنبه طبیعی در فعالیت روزمره هر کارمند تبدیل می‌شود (Schlienger & Tufel 2003). «کوسیستو و ایلونن» بیان می‌کنند: «وحدت ارزش‌های همه بخش‌ها با روند شکل‌گیری فرهنگ امنیت در گیرند». آن‌ها همچنین بیان می‌کنند که اگر ارزش‌های اعضای کل سازمان متحد شود، در کمتر از چند سال فرهنگ واحدی می‌تواند شکل

1. Schein

2. artefacts

بگیرد. با این حال، اگر ارزش اعضای کل سازمان یکپارچه نباشد، روند می‌تواند به‌طور قابل توجهی طولانی‌تر شود (Kuusisto & Ilvonen 2003). «انگو، ژو و وارن» از فرهنگ امنیت اطلاعات به‌عنوان «چگونگی انجام کارها (به‌عنوان مثال، رفتارها و اقدامات پذیرفته‌شده) توسط کارمندان و سازمان به‌عنوان یک کل، در رابطه با امنیت اطلاعات» یاد می‌کنند (Ngo, Zhou & Warren 2005). «دهیلون» فرهنگ امنیتی را چنین تعریف می‌کند: «مجموع ویژگی‌های انسانی همچون رفتارها، نگرش‌ها و ارزش‌هایی که به محافظت از انواع اطلاعات در یک سازمان معین کمک می‌کند» (Dhillon 2006). «مکل‌ریث» فرهنگ امنیت اطلاعات را باور فردی کارمندان در مورد ارزش انطباق با استانداردها و سیاست‌های امنیت اطلاعات تعریف می‌کند» (McIlwraith 2006). «الهوگیل و میرزا» فرهنگ امنیت اطلاعات را مجموعه‌ای از ادراکات، نگرش‌ها، ارزش‌ها، فرضیات و دانش می‌دانند که تعامل انسان با دارایی‌های اطلاعاتی در یک سازمان را با هدف تأثیرگذاری بر رفتار کارکنان برای حفظ امنیت اطلاعات هدایت می‌کند» (AlHogail & Mirza 2015).

همان‌طور که مطرح شد، تعاریف مختلف زیادی از فرهنگ امنیت اطلاعات وجود دارد. «روحونیا و اوفوف» در تحلیل انتقادی خود شانزده تعریف اصلی از فرهنگ امنیت اطلاعات را در ادبیات مربوطه شناسایی کردند و این تعاریف را به‌صورت موضوعی در چهار دیدگاه فرهنگ امنیت اطلاعات، یعنی دیدگاه ارزش مشترک، دیدگاه مبتنی بر عمل، دیدگاه مدل ذهنی، و دیدگاه حل مسئله طبقه‌بندی کردند (Ruhwanya & Ophoff 2019).

تحقیقات بسیاری در زمینه فرهنگ امنیت اطلاعات وجود دارد که جنبه‌های مختلفی از آن را بررسی می‌کنند. برخی محققان همچون (Tang, Van Niekerk & Von Solms 2010)، (Li & Zhang 2016) و (Solomon and Brown 2020) رابطه بین فرهنگ امنیت اطلاعات و فرهنگ سازمانی را بررسی کردند. (Chia, Maynard & Ruighaver, Maynard & Chang 2007) (2002) Ruighaver چارچوبی بر اساس ابعاد فرهنگ سازمانی پیشنهاد نمودند و بر افزایش آگاهی امنیت اطلاعات در سازمان متمرکز بودند تا تأثیر فرهنگ سازمانی بر فرهنگ امنیت اطلاعات را بررسی نمایند. (Sas et al. 2021) و (Shkariet et al. 2020)، (Alnatheer 2014) ارزیابی و اندازه‌گیری فرهنگ امنیت اطلاعات را مورد بررسی قرار دادند. (Da Veiga & Eloff 2010) چارچوبی برای ارزیابی و ارتقای فرهنگ امنیت اطلاعات به‌طور عملی در سازمان‌ها ارائه کردند.

محققان دیگری در پژوهش‌های خود بر روی تعیین ابعاد و عوامل فرهنگ امنیت اطلاعات تمرکز کردند (Sherif & Furnell 2015; Nel & Drevin 2019; Arbanas, Spremic & Hrustek 2021). همچنین محققانی همچون (Van Niekerk & Von Solms (2010) و Mahfuth et al. (2017) بر روی توسعه مدل‌های مفهومی کار کردند و نشان دادند که رابطه مثبتی بین سطوح دانش و رفتار کارکنان وجود دارد. (Nasir, Arshah, AlHogail & Mirza (2015) و (2017) Hamid & Tollah, Furnell & Papadaki، چارچوبی برای فرهنگ امنیت اطلاعات پیشنهاد کردند و (Schlienger & Teufel (2003)، (Chen, Martins & da Veiga (2015) و (2015) Ramamurthy & Wen، (2015) Sherif & Furnell و (2019) در تحقیقات خود در زمینه فرهنگ امنیت اطلاعات مدل ارائه نمودند و نتایجی از چارچوب‌ها و مدل‌های پیشنهادی خود استخراج کردند. (Cheng & Lin (2007) چارچوبی برای تست رابطه میان فرهنگ سازمانی و مدیریت امنیت اطلاعات، و (Alnathier & Nelson (2009) چارچوبی با هدف درک فرهنگ امنیت اطلاعات و بهترین اقدامات صورت گرفته در عربستان سعودی ارائه نمودند. (Chen, Ramamurthy & Wen (2015) مدلی تحقیقاتی برای بررسی تأثیر برنامه‌های آگاهی امنیت اطلاعات با توجه به ایجاد فرهنگ امنیتی پیشنهاد نمودند. (Alfawaz, Nelson & Mohannak (2010) چارچوبی جهت شناسایی ویژگی‌های فرهنگ سازمانی مشروط به شیوه‌های امنیت اطلاعات پیشنهاد نمود. (Dojkovski, Lichtenstein & Warren (2007) چارچوبی جهت بهبود پیاده‌سازی فرهنگ امنیت اطلاعات در شرکت‌های با اندازه کوچک و متوسط ارائه نمودند. (Lim et al. (2010) چارچوبی ارائه نمودند که به سازمان‌ها کمک می‌کند تعیین نمایند آیا فرهنگ امنیت اطلاعات مورد نیاز در فرهنگ سازمان گنجانده شده است یا خیر. برخی از مدل‌ها و چارچوب‌های ارائه شده همچون (Shahri, Ismail & Rahim (2013) در حوزه سلامت ارائه شده است که چارچوبی جامع برای ایجاد امنیت مؤثر برای سیستم‌های اطلاعات سلامت بر اساس فرهنگ امنیتی و آگاهی امنیتی هستند. (Hassan & Ismail (2012) یک مدل مفهومی به‌طور خاص برای محیط مراقبت سلامتی ارائه نمودند.

همچنین، تعدادی از پژوهش‌های مروری مرتبط با فرهنگ امنیت اطلاعات از جمله (AlHogail & Mirza (2015), (Alnathier (2014), (Karlsson & Astrom (2015), (Hassan, Ismail & Maarop (2015) و (Da Veiga et al. (2020) انجام گرفته و این نتیجه به‌دست آمده که تحقیقات موجود عمدتاً نظری یا توصیفی هستند و در شناسایی عوامل و اندازه‌گیری تأثیر

آن بر فرهنگ امنیت اطلاعات کمبود دانش وجود دارد.

پژوهش‌های ذکر شده تعدادی از پژوهش‌های انجام شده در حوزه فرهنگ امنیت اطلاعات هستند و طی دو دهه اخیر مطالعات بسیاری در این حوزه صورت گرفته است که با مرور نظام‌مند بررسی و تحلیل می‌شوند تا ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات شناسایی گردد. این مطالعات نشان می‌دهند که فرهنگ امنیت اطلاعات محصول طیف گسترده‌ای از عوامل است که در کنار هم برای اتخاذ یک استراتژی جامع مدیریتی که مناسب دیده می‌شود، تأثیر گذارند. بر اساس این دغدغه، برای شناخت ابعاد موضوع و بررسی پژوهش‌های قبلی انجام شده، در این مقاله پژوهش‌ها به صورت نظام‌مند مرور شده و نکات مورد توجه که می‌توانند در پژوهش‌های آتی راهگشا باشند، استخراج شده و در قالب جدول و نمودارهای کمی و کیفی ارائه شده‌اند. در ادامه مقاله، در بخش ۲، روش تحقیق اتخاذ شده در این پژوهش ارائه می‌گردد. در بخش ۳، تجزیه و تحلیل و یافته‌ها بیان می‌شود و در بخش ۴، نتیجه‌گیری ارائه می‌گردد.

۲. روش تحقیق

هدف مقاله حاضر شناسایی ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات است. بدین منظور، لازم است پژوهش‌های انجام شده در زمینه فرهنگ امنیت اطلاعات به طور جامع بررسی گردند. برای این منظور از روش مرور نظام‌مند استفاده شده است. مرور نظام‌مند به مطالعاتی اطلاق می‌شود که با یافتن، توصیف و ارزیابی همه تحقیقات منتشر شده و در صورت امکان منتشر نشده در مورد یک موضوع، به دنبال پاسخ به یک سؤال یا سؤالات روشن هستند. مرورهای نظام‌مند با مرورهای ادبیات سنتی که اغلب به عنوان بررسی‌های روایی شناخته می‌شوند، متفاوت است (Al-Tabbaa, Ankrah & Zahoor 2019). مرور نظام‌مند روشی است که به طور معمول، برای به دست آوردن یک نمای کلی از یک مقیاس خاص و جمع آوری و تجزیه و تحلیل داده‌ها از یک سری مطالعات استفاده می‌شود. این روش، ارزیابی انتقادی از مقیاس‌های شناسایی شده را امکان‌پذیر ساخته و یافته‌ها به بهینه‌سازی بیشتر آن مقیاس‌ها کمک می‌کند (Moher et al. 2009). از آنجا که مطالعات فردی می‌تواند پراکنده باشد و تنها یک جنبه از یک تصویر بزرگ‌تر را نشان دهد، ارزش یک مرور نظام‌مند این است که قطعات گسسته را ترکیب می‌کند و نتایج را به روشی سازمان یافته ترکیب می‌کند و اجازه می‌دهد که یک نمای کلی از

موضوع مورد تحقیق مشاهده شود. محقق با انجام یک مرور نظام‌مند ادبیات می‌تواند شواهد موجود در مورد یک پدیده را خلاصه کند، شکاف‌های موجود در تحقیقات فعلی را شناسایی کرده و چارچوبی را برای موضع یا حمایت از ایده‌ها و فرضیه‌های جدید ارائه دهد (Silva 2015).

با توجه به هدف این مقاله، مرور نظام‌مند انجام‌شده مبنایی نظری برای شناسایی ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات فراهم می‌کند و به سؤال اصلی این تحقیق که «چه مؤلفه‌هایی بر فرهنگ امنیت اطلاعات تأثیر گذارند؟» پاسخ می‌دهد. بدیهی است برای آنکه این مسیر به‌درستی طی گردد، باید پروتکلی دقیق، تعریف و تعیین گردد. پروتکل، واژگان جست‌وجو، معیارهای ورود و خروج، داده‌هایی که باید تحلیل گردند و ... را تعریف می‌کند. جزئیات هر یک از مراحل که پروتکل را تشکیل می‌دهند در ادامه این مقاله توضیح داده شده است.

استراتژی جست‌وجو

مرور نظام‌مند ادبیات با استفاده از پایگاه‌های اطلاعاتی مقالات خارجی برای جمع‌آوری مقالات مرتبط با فرهنگ امنیت اطلاعات انجام شد. پایگاه داده‌های مورد استفاده برای جست‌وجوی مطالعات در این تحقیق SPRINGER، IEEE، SAGE، ELSEVIER/ScienceDirect و Emerald بودند. برای اطمینان بیشتر از اینکه هیچ مقاله مهم و مرتبطی از دست نرفته است، جست‌وجو در Google Scholar نیز انجام گرفت. برای جست‌وجو از کلمات کلیدی "information security culture"، "security culture" و "culture of information security" استفاده گردید.

شناسایی

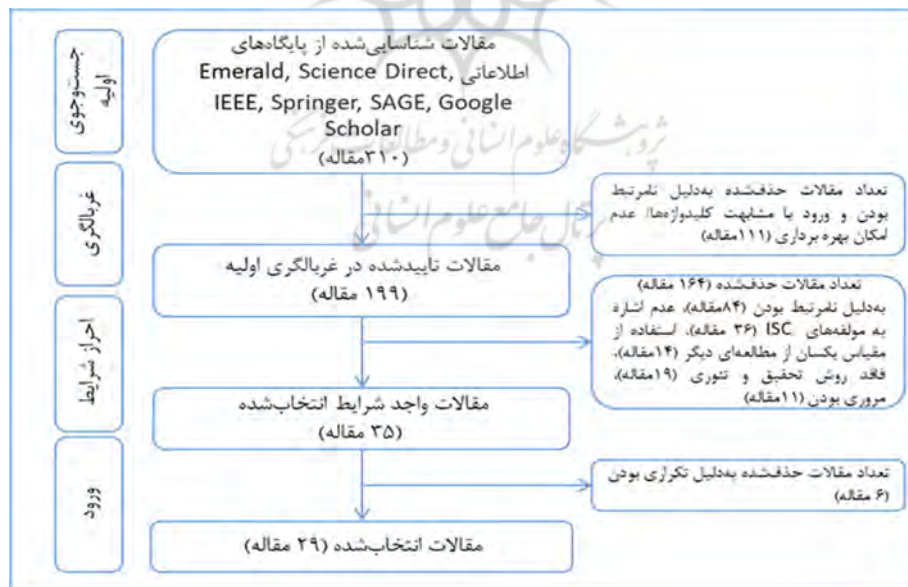
جست‌وجو در پایگاه‌های اطلاعاتی با کلمات کلیدی منتخب در عنوان، چکیده و کلمات کلیدی مقالات صورت گرفت. در تعیین حدود جست‌وجو، تنها محدودیت عمده‌ای که برای جست‌وجو در پایگاه‌ها اعمال شد، محدودیت زبان بود. بر این اساس، تنها زبان مورد جست‌وجو انگلیسی بود و کلیه مقالات ژورنالی و کنفرانسی در طی سال‌های ۲۰۰۰ تا ۲۰۲۲ استخراج گردید. سایر محدودیت‌های قابل به‌کارگیری از قبیل ناحیه موضوعی، کشور، نویسنده و سایر محدودیت‌های ممکن اعمال نشد. هدف از این کار، گردآوری حداکثر ممکن مستندات بود. بر این اساس تعداد ۳۱۰ مقاله از پایگاه‌های اطلاعاتی یافت شد.

انتخاب و ارزیابی مقالات

ارزیابی صلاحیت برای درج یا حذف مقالات در این بررسی در چهار مرحله به شرح زیر انجام شد. به منظور انتخاب و ارزیابی مقالات، در گام اول، برای تعیین و انتخاب عناوین مرتبط، با جست‌وجوی سریع اصطلاحات تحقیق در عنوان، چکیده و کلید واژگان، مقالاتی که هیچ‌یک از اصطلاحات تحقیق را شامل نمی‌شدند، حذف گردیدند. در این مرحله تعداد ۱۱۱ مقاله حذف گردید.

در گام دوم، برای ارزیابی مقالات با مرور کل مقاله، با توجه به اینکه هدف مرور، شناسایی مؤلفه‌های فرهنگ امنیت اطلاعات است، از مجموع مقالات، تعداد ۱۶۴ مقاله به دلایل مختلف زیر حذف گردید: نامرتب بودن مقاله (۸۴ مقاله)، مقالات نظری، بدون تحقیق تجربی و روش تحقیق (۱۹ مقاله)، عدم اشاره به مفهوم فرهنگ امنیت اطلاعات و یا عدم اشاره به مؤلفه، شاخص یا مدل (۳۶ مقاله)، استفاده از مقیاس‌های یکسان از نویسندگان دیگر (۱۴ مقاله) و مقالات مروری (۱۱ مقاله).

در گام آخر با حذف مقالات مشابه و تکراری (۶ مقاله) تعداد ۲۹ مقاله برای مرور نهایی و انجام تجزیه و تحلیل انتخاب گردید. شکل ۱، فرایند جست‌وجوی نظام‌مند و تعداد ورود و خروج مقالات را نشان می‌دهد.



شکل ۱. فرایند جست‌وجوی نظام‌مند و ورود و خروج مقالات در مرور

۳. تجزیه و تحلیل و یافته‌ها

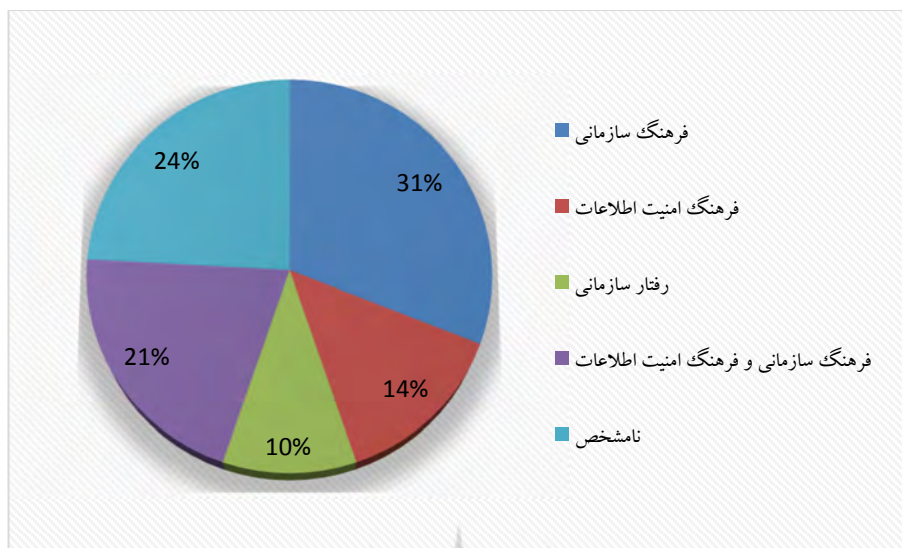
بر اساس مرور نظام‌مند، تحقیقاتی مورد توجه قرار گرفتند که به‌طور مشخص به موضوع فرهنگ امنیت اطلاعات پرداخته‌اند؛ بدین صورت که به بررسی مفهوم فرهنگ امنیت اطلاعات پرداخته‌اند، چارچوب یا مدلی برای فرهنگ امنیت اطلاعات ارائه نموده‌اند و یا ابزاری جهت ارزیابی فرهنگ امنیت اطلاعات ارائه و پیشنهاد داده‌اند. بر این اساس و به دنبال بررسی مقالات منتخب در مرور نظام‌مند، نتایج و یافته‌های زیر حاصل گردید.

تئوری‌های استفاده‌شده در پژوهش‌ها

با توجه به داده‌های استخراج‌شده از مقالات، مدل‌ها و چارچوب‌های موجود بر اساس ۳ مفهوم رفتار سازمانی، فرهنگ سازمانی، و فرهنگ امنیت اطلاعات و یا بدون اشاره به مفهوم و تئوری خاص و با مرور ادبیات توسعه یافته‌اند. مقالات توسعه یافته بر اساس فرهنگ سازمانی بیشتر، از مدل فرهنگ سازمانی «شاین»^۱ بهره برده‌اند و تنها تحقیق Tang, Li & Zhang (2016) از مدل فرهنگ سازمانی «هافستد»^۲ به‌عنوان تئوری مبنا استفاده نموده است. مفهوم فرهنگ امنیت اطلاعات به‌عنوان زیرفرهنگی از فرهنگ سازمانی از تحقیقات Van Niekerk and Von Solms (2006) توسعه یافته است و در واقع، لایه دانش به مدل «شاین» افزوده شده است و به‌عنوان مبنایی برای تحقیقات حوزه امنیت اطلاعات استفاده می‌گردد. در شکل ۲، میزان و درصد تئوری‌های به کار برده‌شده در تحقیقات نشان داده شده است.

1. Schein

2. Hofstede



شکل ۲. فراوانی تئوری‌های استفاده شده در تحقیقات

انواع روش‌های به‌کاررفته در پژوهش‌ها

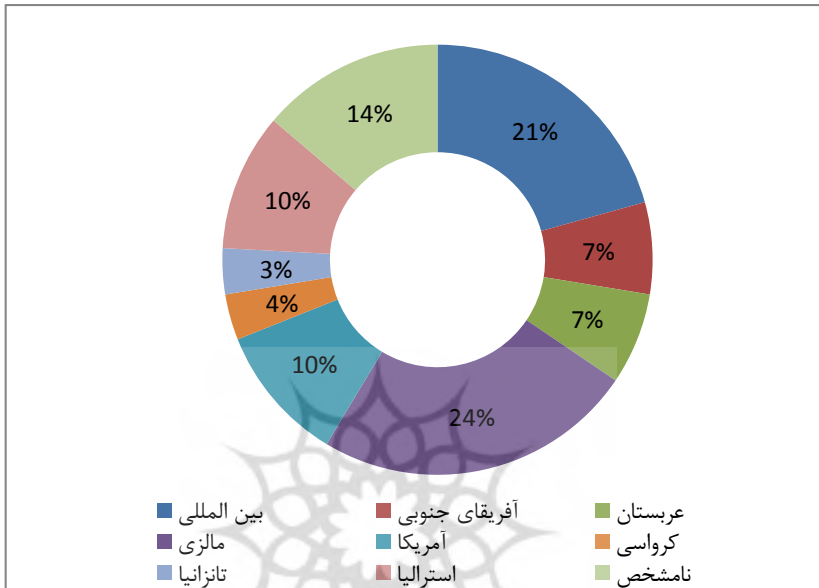
با توجه به اینکه در انتخاب مقالات، استفاده از انواع تحقیق، شیوه‌های جمع‌آوری داده و تجزیه و تحلیل داده‌ها توسط ابزارها ملاک قرار گرفته، از این رو، نوع تحقیق مقالات منتخب شیوه‌های کمی، کیفی و یا ترکیبی از دو روش است. ابزار جمع‌آوری داده‌ها در تحقیقات بهره‌گیری از پرسشنامه، مصاحبه و یا ترکیبی از این دو متناسب با نوع تحقیق بوده است. از این میان، ۵۲ درصد از تحقیقات به صورت کمی، ۲۸ درصد به صورت کیفی و ۲۱ درصد به صورت ترکیبی انجام گرفته است.

پژوهش‌های فرهنگ امنیت اطلاعات از نظر روش تحلیل داده‌ها و نرم‌افزارهای به‌کاررفته در تحلیل داده نیز بررسی شدند. مدل‌سازی معادلات ساختاری مبتنی بر واریانس و کواریانس، تحلیل عاملی، و تحلیل شاخص‌های برازش جزء پرتکرارترین روش‌های استفاده شده بودند. همچنین برای تحلیل داده از ابزارها و نرم‌افزارهای SPSS، SmartPLS، Excel، MPIus، Survey Tracker و Atlas-ti استفاده شده است.

تمرکز جغرافیایی پژوهش‌ها

بر اساس پژوهش‌های بررسی‌شده و کشورهای که پژوهش روی آن‌ها تمرکز دارد،

می‌توان توزیع جغرافیایی پژوهش‌ها را نشان داد. بررسی پژوهش‌ها حاکی از آن است که بیشتر این تحقیقات در کشورهای در حال توسعه صورت گرفته است. شکل ۳، توزیع جغرافیایی پژوهش‌ها را نشان می‌دهد.



شکل ۳. توزیع جغرافیایی پژوهش‌ها

ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات

به دنبال بررسی مقالات منتخب در مرور نظام‌مند، از آنجا که پرسش اصلی این پژوهش شناسایی مؤلفه‌های فرهنگ امنیت اطلاعات است، کلیه ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات شناسایی شده در تحقیقات مختلف، بر اساس دیدگاه‌های مختلف گردآوری و در جدول ۱، آورده شده است.

جدول ۱. ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات

ردیف	مؤلفه‌ها	نویسندگان و سال انتشار
۱	چشم‌انداز و اهداف امنیتی	Da veiga & Martins 2017; Hassan, Maarop & Esmail 2017
۲	سیاست‌ها و رویه‌های امنیتی	Da veiga et al. 2020; Da veiga & Ellof 2010; Da veiga & Martins 2014; Da veiga & Martins 2015; Da veiga & Martins 2017; Tollah, Furnell & Papadaki 2021; Tollah, Furnell & Papadaki 2019; Nel & Drevin 2019; Mahfuth 2017; Chen, Ramamurthy & Wen 2015; Martins & Ellof 2002; Ruhwanya & Ophoff 2019; Masrek, Harun & Zaini 2018; Arbanas, Spremic & Hrustek 2021; Dojkovski, Lichtenstein & Warren 2006
۳	راهنماهای امنیت اطلاعات	Da veiga & Ellof 2010
۴	گواهینامه‌های امنیتی	Da veiga & Ellof 2010
۵	بهبودها	Da veiga & Ellof 2010
۶	اقدامات فنی جهت حفظ محرمانگی	Da veiga et al. 2020; Arbanas, Spremic & Hrustek 2021
۷	اقدامات فنی جهت در دسترس بودن و حفاظت سیستمی از اطلاعات	Da veiga et al. 2020; Arbanas 2021
۸	اقدامات فنی جهت حفظ یکپارچگی	Da veiga et al. 2020; Arbanas, Spremic & Hrustek 2021
۹	سیستم‌ها و فرایندهای امنیتی مناسب	Hassan et al. 2017; Mahfuth 2017
۱۰	مدیریت دارایی اطلاعات	Da veiga & Ellof 2010; Da veiga & Martins 2014; Da veiga & Martins 2015; Nel & Drevin 2019

نویسندگان و سال انتشار	مؤلفه‌ها	ردیف
Masrek, Harun & Zaini 2018	IT capability	۱۱ قابلیت فناوری اطلاعات
Masrek, Harun & Zaini 2018	IT Compatibility	۱۲ سازگاری فناوری اطلاعات
Da veiga & Ellof 2010; Nel & Drevin 2019	incident management	۱۳ مدیریت رخداد
Da veiga & Ellof 2010; Ruhwanya & Ophoff 2019	international security standards	۱۴ استانداردهای امنیت بین‌المللی
Da veiga & Ellof 2010; Nel & Drevin 2019	business continuity plan	۱۵ برنامه تداوم کسب و کار
Tollah, Furnell & Papadaki 2021; Tollah, Furnell & Papadaki 2019; Hassan & Esmail 2017; Kraemer & carayon 2005; Arbanas, Spremic & Hrustek 2021; D'Arcy & Greene 2014; Alnatheer, Chan & Nelson 2012; Nasir, Arshah & hamid, 2019; Nasir, Arshah & hamid, 2020; Nasir, Rashid & Hamid, 2018 Lim et al. 2010; Ruhwanya & Ophoff 2019; Dojkovski, Lichtenstein & Warren 2007; Masrek, Harun & Zaini 2018	top management commitment, involvement & support	۱۶ تعمد، مشارکت و حمایت مدیریت ارشد
Lim et al. 2010; Martins & Ellof 2002; Masrek, Harun & Zaini 2018; Dojkovski, Lichtenstein & Warren 2006	allocation budget for information security	۱۷ تخصیص بودجه برای امنیت اطلاعات
Da veiga & Ellof 2010; Nel & Drevin 2019	ROI	۱۸ نرخ بازگشت حاصل از سرمایه‌گذاری در IS

نویسندگان و سال انتشار	مؤلفه‌ها	ردیف
Da veiga et al. 2020; Da veiga & Ellof 2010; Da veiga & Martins 2014; Da veiga & Martins 2015; Da veiga & Martins 2017; Alhogail 2015; Hassan & Esmail 2017; Nel & Drevin 2019; Mahfuth et al. 2017; Dojkovski, Lichtenstein & Warren 2006	change management	مدیریت تغییر ۱۹
Da veiga et al. 2020; Da veiga & Ellof 2010; Tollah, Furnell & Papadaki 2021; Tollah, Furnell & Papadaki 2019; Nel & Drevin 2019; Nasir, Arshah & hamid 2019; Nasir, Arshah & hamid 2020; Nasir, Rashid & Hamid 2018 Mahfuth et al. 2017; Martins & Ellof 2002; Ruhwanya & Ophoff 2019; Dojkovski, Lichtenstein & Warren 2006	security risk analysis and assessment	ارزیابی و تحلیل ریسک امنیتی ۲۰
Kraemer & carayon 2005	hiring practices	اقدامات استخدامی ۲۱
Kraemer & carayon 2005	reward system	سیستم پاداش ۲۲
Da veiga et al. 2020; Da veiga & Martins 2017; Hassan & Esmail 2017; Hassan et al. 2017; Nasir, Arshah & hamid 2019; Nasir, Arshah & hamid 2020; Nasir, Rashid & Hamid 2018 Mahfuth et al. 2017; Dojkovski, Lichtenstein & Warren 2006	knowledge management	مدیریت دانش ۲۳
Da veiga et al. 2020	internal state of the organization (stability, dynamism, business activity)	وضعیت داخلی سازمان ۲۴
Da veiga et al. 2020	life cycle state of organization	وضعیت چرخه عمر سازمان ۲۵
Da veiga et al. 2020; Da veiga & Martins 2017; Dojkovski, Lichtenstein & Warren 2007; Dojkovski, Lichtenstein & Warren 2006	organizational culture	فرهنگ سازمانی ۲۶

ردیف	مؤلفه‌ها	نویسندگان و سال انتشار
۲۷	برنامه‌های آگاهی، آموزشی و یادگیری (SETA) امنیتی	Da veiga et al. 2020; security education, training and Da veiga & Ellof 2010; awareness programs (SETA) Da veiga & Martins 2014; Da veiga & Martins 2015; Da veiga & Martins 2017; Tollah, Furnell & Papadaki 2021; Tollah, Furnell & Papadaki 2019; Kraemer & carayon 2005; Nel & Drevin 2019; Azmi et al. 2021; Arbanas, Spremic & Hrustek 2021; Alnatheer, Chan & Nelson 2012; Nasir, Arshah & hamid 2019; Nasir, Arshah & hamid 2020; Nasir, Rashid & Hamid 2018; Chen, Ramamurthy & Wen 2015; Lim et al. 2010; Ruhwanya & Ophoff 2019; Dojkovski, Lichtenstein & Warren 2006 Mahfuth et al. 2017; Masrek, Harun & Zaini 2018
۲۸	آگاهی از امنیت اطلاعات	Da veiga et al. 2020; information security awareness Da veiga & Ellof 2010; Da veiga & Martins 2017; Hassan et al. 2017; Nel & Drevin 2019; Azmi et al. 2021; Arbanas, Spremic & Hrustek 2021; Mahfuth 2017; Lim et al. 2010; Martins & Ellof 2002; Dojkovski, Lichtenstein & Warren 2007; Dojkovski, Lichtenstein & Warren 2006; Tollah, Furnell & Papadaki 2021; Tollah, Furnell & Papadaki 2019; Nel & Drevin 2019
۲۹	مدیریت رفتار امنیتی کارکنان	Da veiga et al. 2020; employees' information security Da veiga & Martins 2017; behavior management Azmi et al. 2021

نویسندگان و سال انتشار	مؤلفه‌ها	ردیف
Hassan & Esmail 2017; Lim et al. 2010; Alnatheer 2012	security policy enforcement	اجرای سیاست‌های امنیت s ۳۰
D'Arcy & Greene 2014; Nasir, Arshah & hamid, 2019; Nasir, Arshah & hamid, 2020; Nasir, Rashid & Hamid, 2018; Chen, Ramamurthy & Wen, 2015; Dojkovski, Lichtenstein & Warren 2007; Masrek, Harun & Zaini 2018; Nel & Drevin 2019	security monitoring and audit	نظارت و ممیزی امنیتی ۳۱
Da veiga et al. 2020; Da veiga & Ellof 2010; Alhogail 2014; Alhogail 2015; Tang, Li & Zhang 2016	management and governance	مدیریت و حاکمیت ۳۲
Hassan & Esmail 2017	information security needs determining	تعیین نیازهای IS ۳۳
Da veiga & Ellof 2010; Da veiga & Martins 2014; Da veiga & Martins 2015; Nel & Drevin 2019	Information security program	برنامه IS ۳۴
Kraemer & carayon 2005; D'Arcy 2014; Tang, Li & Zhang 2016; Nel & Drevin 2019	security communication and feedback	ارتباط و بازخورد امنیتی ۳۵
Da veiga et al. 2020; Da veiga & Ellof 2010; Da veiga & Martins 2014; Da veiga & Martins 2015; Nel & Drevin 2019; Mahfuth 2017; Martins & Ellof 2002; Dojkovski, Lichtenstein & Warren 2006	mutual trust of the management & employees	اعتماد متقابل مدیریت و کارمندان ۳۶
Da veiga et al. 2020; Nel & Drevin 2019	fulfillment of personal needs of employees	برآوردن نیازهای کارکنان ۳۷
Tollah, Furnell & Papadaki 2021; Tollah, Furnell & Papadaki 2019	personality trait	ویژگی‌های شخصیتی ۳۸

نویسندگان و سال انتشار	مؤلفه‌ها	ردیف
Tollah, Furnell & Papadaki 2021; Tollah, Furnell & Papadaki 2019	job satisfaction	۳۹ رضایت شغلی
Arbanas, Spremic & Hrustek 2021; Mahfuth et al. 2017	beliefs	۴۰ باورها
Alhogail 2015; Tang, Li & Zhang 2016; Masrek, Harun & Zaini 2018; Nel & Drevin 2019; Dojkovski, Lichtenstein & Warren 2006; Lim et al. 2010; Mahfuth 2017	accountability & responsibility	۴۱ مسئولیت پذیری و پاسخگویی
Hassan & Esmail 2017; Dojkovski, Lichtenstein & Warren 2006	collaboration and cooperation	۴۲ همکاری و مشارکت
Da veiga et al. 2020; Dojkovski, Lichtenstein & Warren 2006	values	۴۳ ارزش‌ها
Dojkovski, Lichtenstein & Warren 2006	motivation	۴۴ انگیزه
Dojkovski, Lichtenstein & Warren 2006	personal growth	۴۵ رشد فردی
Tollah, Furnell & Papadaki 2021; Tollah, Furnell & Papadaki 2019; Nel & Drevin 2019; Mahfuth 2017; Martins & Ellof 2002; Dojkovski, Lichtenstein & Warren 2006; Da veiga & Ellof 2010	ethicity& ethical conduct	۴۶ اخلاقیات و رفتارهای اخلاقی
Da veiga & Martins 2017; Alhogail 2014; Alhogail 2015; Mahfuth 2017; Nel & Drevin 2019; Da veiga & Ellof 2010	legal and regulatory requirements	۴۷ الزامات بالادستی و قانونی
Ruhwanya & Ophoff 2019; Dojkovski, Lichtenstein & Warren 2007	IT suppliers, vendors & Partners	۴۸ فروشندگان و عرضه کنندگان IT و همکاران

نویسندگان و سال انتشار	مؤلفه‌ها	ردیف
Da veiga et al. 2020; Da veiga & Martins 2017; Ruhwanya & Ophoff 2019; Dojkovski, Lichtenstein & Warren 2006; Dojkovski, Lichtenstein & Warren 2007	national culture	فرهنگ ملی ۴۹
Tang, Li & Zhang 2016; Dojkovski, Lichtenstein & Warren 2007	government	دولت و حاکمیت ۵۰
Da veiga et al. 2020	economic	اقتصاد ۵۱
Da veiga et al. 2020; Arbanas, Spremic & Hrustek 2021	social culture	فرهنگ اجتماعی ۵۲

محققان مختلف از منظرهای مختلفی به موضوع فرهنگ امنیت اطلاعات پرداخته‌اند. برخی محققان از تئوری‌های فرهنگ سازمانی برای شناسایی و دسته‌بندی مؤلفه‌های تأثیرگذار بر فرهنگ امنیت اطلاعات بهره برده‌اند و برخی از تئوری فرهنگ امنیت اطلاعات و برخی دیگر از تئوری‌های رفتار سازمانی بهره برده‌اند و بر این اساس مؤلفه‌های موجود و شناسایی شده خود را دسته‌بندی نموده‌اند. در برخی پژوهش‌ها عوامل تأثیرگذار بر فرهنگ امنیت اطلاعات به ابعاد و عوامل داخلی و خارجی سازمان دسته‌بندی، و مؤلفه‌ها ذیل این ابعاد ذکر شده‌اند. مؤلفه‌های ذکر شده در جدول فوق، مؤلفه‌هایی هستند که در تحقیقات مختلف از آن‌ها به‌عنوان مؤلفه‌های تأثیرگذار بر فرهنگ امنیت اطلاعات نام برده شده است. از این‌رو، مؤلفه‌های مختلف از پژوهش‌های مختلف صورت گرفته در سال‌های گذشته استخراج شده‌اند تا این عوامل تأثیرگذار به‌صورت مجتمع و گردآوری شده، مورد بهره‌برداری قرار گیرد و شکاف دانشی موجود در زمینه مؤلفه‌های فرهنگ امنیت اطلاعات را برطرف نماید.

همان‌طور که مشهود است، مؤلفه‌های متعدد و مختلفی در پژوهش‌های مختلف مورد استفاده قرار گرفته‌اند و محققان مختلف بر اساس دیدگاه خود برخی از مؤلفه‌ها را بیان نموده‌اند و بنابراین، اجماعی در این حوزه وجود ندارد. به‌رغم نبود اجماع نسبت به مؤلفه‌های فرهنگ امنیت اطلاعات، برخی مؤلفه‌ها در بسیاری از پژوهش‌ها بسیار تکرار شده‌اند و به‌عنوان مؤلفه‌های اساسی در چارچوب یا مدل‌های ارائه شده در نظر گرفته شده‌اند. همچنین، در برخی پژوهش‌ها به‌عنوان عوامل سازنده فرهنگ امنیت اطلاعات

عنوان شده‌اند و به‌عنوان عوامل ارزیابی فرهنگ امنیت اطلاعات از آن‌ها استفاده گردیده است. برخی از این مؤلفه‌های پرتکرار عبارت‌اند از: سیاست‌ها و رویه‌های امنیتی، تعهد، مشارکت و حمایت مدیریت ارشد، مدیریت تغییر، ارزیابی و تحلیل ریسک امنیتی، فرهنگ سازمانی، مدیریت دانش، برنامه‌های آگاهی، آموزشی و یادگیری امنیتی (SETA)، آگاهی از امنیت اطلاعات، مسئولیت‌پذیری و پاسخگویی، اخلاقیات و رفتارهای اخلاقی، اعتماد متقابل مدیریت و کارمندان، الزامات بالادستی^۱ و قانونی، ارتباط و بازخورد امنیتی، نظارت و ممیزی امنیتی.

۴. نتیجه‌گیری

تحقیقات مختلفی در حوزه فرهنگ امنیت اطلاعات صورت گرفته و هر یک از محققان مختلف، از جنبه‌ای به این موضوع پرداخته‌اند. برخی از مطالعات از مؤلفه‌های شناسایی شده در سایر تحقیقات استفاده نمودند؛ برخی رابطه میان فرهنگ امنیت اطلاعات و سایر عوامل همچون فرهنگ سازمانی و رفتار سازمانی را بیان نموده‌اند و یا با پیش‌فرض رفتار انسانی، تنها به دنبال عوامل انسانی تأثیرگذار بودند و از این دیدگاه، مؤلفه‌هایی را به‌عنوان عوامل سازنده یا تأثیرگذار فرهنگ امنیت معرفی نموده‌اند و یا آن‌ها را برای ارزیابی فرهنگ امنیت اطلاعات در نظر گرفته‌اند؛ برخی محققان در تحقیقات خود چارچوب‌ها و مدل‌هایی ارائه کرده و به‌رغم اینکه بسیاری از مؤلفه‌ها را در مدل یا چارچوب خود در نظر گرفته‌اند، تنها جنبه تئوری و توصیفی دارند و مورد سنجش قرار نگرفته‌اند؛ برخی محققان نیز از مؤلفه‌های تحقیقات خود و سایر تحقیقات انجام‌شده استفاده نموده و مدل‌هایی را برای ارزیابی فرهنگ امنیت اطلاعات ارائه نموده‌اند که در کل، مؤلفه‌های محدودی را در نظر گرفته و از لحاظ نمودن بسیاری از مؤلفه‌ها در مدل ارزیابی پیشنهادی خود چشم‌پوشی کرده‌اند.

بر اساس تحقیق صورت گرفته در این مقاله آشکار گردید که در اکثر تحقیقات صورت گرفته در این زمینه، تنها به بخشی از فرهنگ امنیت اطلاعات پرداخته شده و بر اساس جنبه‌ای خاص، مؤلفه‌هایی در نظر گرفته شده است و این امر سبب شده است که در بسیاری از تحقیقات برخی مؤلفه‌ها لحاظ نگردد. از آنجا که موضوع فرهنگ امنیت

1. security education, training and awareness programs (SETA)

2. regulatory requirements

اطلاعات موضوعی چندوجهی است و نمی‌توان به آن تنها از دید عامل انسانی و رفتار آن و یا فرهنگ سازمانی و یا حتی فناوری نگریست، بنابراین، بررسی آن از جنبه‌های مختلف ضروری است و به‌عنوان یکی از نتایج این مرور می‌توان به شناسایی شکاف مذکور در مطالعات صورت گرفته و لزوم انجام بررسی‌های بیشتر در زمینه فرهنگ امنیت اطلاعات با دیدی همه‌جانبه اشاره نمود.

با توجه به اهمیت این موضوع و مشکلات امنیتی که به‌رغم وجود فناوری‌های پیشرفته همچنان وجود دارد، توجه بیشتر به مبحث فرهنگ امنیت اطلاعات ضروری است. در این پژوهش با مرور پژوهش‌هایی که تاکنون انجام گرفته، مجموعه ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات شناسایی گردید؛ مفاهیم و رویکردهای زیربنایی که بر اساس آن‌ها تحقیقات صورت گرفته، دسته‌بندی شد؛ و رویکرد مطالعات، نوع سازمان‌های مورد مطالعه، و کشورهایی که تحقیقات را انجام داده‌اند، مشخص گردید. تجزیه و تحلیل پژوهش‌ها نشان داد که پژوهش‌ها و مدل‌های حوزه فرهنگ امنیت اطلاعات بر اساس مفاهیم فرهنگ سازمانی، رفتار سازمانی و فرهنگ امنیت اطلاعات که شاخه‌ای از فرهنگ سازمانی است، شکل گرفته و تأثیر گذارترین مدل فرهنگ سازمانی، مدل فرهنگ سازمانی «شاین» است.

این پژوهش نشان داد که ابعاد و مؤلفه‌هایی که به‌عنوان عوامل سازنده یا تأثیرگذار در فرهنگ امنیت اطلاعات در نظر گرفته شده، از نظر تعداد، شکل‌گیری و مفهوم متفاوت هستند و هنوز ابعاد پذیرفته‌شده‌ای برای فرهنگ امنیت اطلاعات وجود ندارد.

پژوهش حاضر به‌منظور شناسایی مؤلفه‌های مختلف در فرهنگ امنیت اطلاعات صورت گرفت و به‌عنوان پژوهشی اولیه در این زمینه است تا در تحقیقات آتی بتوان به کمک این مؤلفه‌ها و دسته‌بندی آن‌ها به مدلی دست یافت تا با در نظر گرفتن کلیه ابعاد، امکان ارزیابی فرهنگ امنیت اطلاعات فراهم آید. همچنین، از آنجا که مفاهیم، ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات هنوز در حال تکامل است، یافته‌های این پژوهش راه را برای مطالعات دیگر مرتبط با فرهنگ امنیت همچون تأثیر عوامل سازمانی، انسانی، فناورانه و ... در آینده هموار می‌سازد.

References

- Alfawaz, S., K. Nelson, & K. Mohannak. 2010. Information security culture: a behaviour compliance conceptual framework. In *Information Security 2010: AISC'10 Proceedings of the Eighth Australasian Conference on Information Security [Conferences in Research and Practice in Information Technology 105]*: 51-60.
- AlHogail, A. 2015. Design and validation of information security culture framework. *Computers in Human Behavior* 49:567-575 .
- Ali, R. F., P. D. D. Dominic, S. E. A. Ali, M. Rehman, & A. Sohail. 2021. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences* 11 (8): 3383.
- Alnatheer, M. A. 2014. A conceptual model to understand information security culture. *International Journal of Social Science and Humanity* 4 (2): 104.
- _____, M., T. Chan, & K. Nelson. 2012. Understanding and measuring information security culture. In *Proceedings of the 16th Pacific Asia Conference on Information Systems (PACIS)* (pp. 1-15). University of Science (Vietnam)/ AIS Electronic Library (AISeL).
- Al-Tabbaa, O., S. Ankrah, & N. Zahoor. 2019. *Systematic literature review in management and business studies: A case study on university-industry collaboration.?*: SAGE Publications Ltd.
- Arbanas, K., M. Spremic, & N. Z. Hrustek. 2021. Holistic framework for evaluating and improving information security culture. *Aslib Journal of Information Management* 73 (5): 699-719.
- Azmi, N. A. A. M., A. P. Teoh, A. Vafaei-Zadeh, & H. Hanifah. 2021. Predicting information security culture among employees of telecommunication companies in an emerging market. *Information & Computer Security?*
- Chen, Y. A. N., K. Ramamurthy, & K. W. Wen. 2015. Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems* 55 (3): 11-19.
- Cheng, Ch. & Y. Lin. 2002. Evaluating the best mail battle tank using fuzzy decision theory with linguistic criteria evaluation. *European Journal of Operational Research* 142: 147-186.
- Chia, P., S. Maynard, & A. B. Ruighaver. 2002b. "Understanding Organisational Security Culture". Paper presented at the Sixth Pacific Asia Conference on Information Systems.
- D'Arcy, J., & G. Greene. 2014. Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security* 22 (5): 474-489.
- Da Veiga, A., & J. H. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & security* 29 (2): 196-207.
- Da Veiga, A., & N. Martins. 2014. Information security culture: A comparative analysis of four assessments. In *Proceedings of the 8th European Conference on IS Management and Evaluation* (Vol. 8, No. 2014, pp. 49-57). Ghent, Belgium.
- 2015 ._____. Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review* 31 (2): 243-256.
- 2017 ._____. Defining and identifying dominant information security cultures and subcultures. *Computers & Security* 70: 72-94.
- Da Veiga, A., L. V. Astakhova, A. Botha, & M. Herselman. 2020. Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security* 92: 101713.
- Dhillon, G. 2006. *Principles of information systems security - text and cases*. Hoboken, NJ.: Wiley.
- Dojkovski, S., S. Lichtenstein, & M. J. Warren. 2007. Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. In *Proceedings of the European Conference on Information Systems (ECIS)*. At. Gallen, Switzerland.

- _____, & M. Warren. 2006. Challenges in fostering an information security culture in Australian small and medium sized enterprises. In *ECIW2006: proceedings of the 5th European conference on Information Warfare and Security*. Academic Conferences Limited (pp. 31-40).
- Dong, K., R. F/ Ali, P. Dominic, S. E. A. Ali. 2021. The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses. *Sustainability* 13 (5): 2800.
- Hassan, N. H., & Z. Ismail. 2012. A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia-Social and Behavioral Sciences* 65: 1007-1012.
- _____, and N. Maarop. 2015. "Information security culture: a systematic literature review", Proceedings of the 5th International Conference on Computing and Informatics, Istanbul, Turkey, pp. 456-463.
- Hassan, N. H., N. Maarop, Z. Ismail, & W. Z. Abidin. 2017. Information security culture in health informatics environment: A qualitative approach. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.
- IBM Infographic: Cyber Security Intelligence Index; IBM: Armonk, NY, USA, 2014. Available online: <http://www-935.ibm.com/services/us/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic>.
- Karlsson, F., J. Åström, & M. Karlsson. 2015. Information security culture—state-of-the-art review between 2000 and 2013. *Information & Computer Security* 23 (3): 246-285.
- Kraemer, S., & P. Carayon. 2005. Computer and information security culture: Findings from two studies. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 49, No. 16, pp. 1483-1488). Los Angeles, CA: SAGE Publications.
- Kuusisto, T., & I. Ilvonen. 2003. Information security culture in small and medium size enterprises. *Frontiers of E-business Research?*: 431-439.
- Lim, J. S., A. Ahmad, S. Chang, & S. Maynard. 2010. Embedding information security culture emerging concerns and challenges. Proceedings of the Pacific Asia Conference on Information Systems, PACIS, Taipei, Taiwan.
- Mahfuth, A., S. Yussof, Asmidar abu Bakar, N. A. B. Ali, & W. Abdallah. 2017. A conceptual model for exploring the factors influencing information security culture. *International Journal of Security and Its Applications* 11 (5): 15-21.
- Martins, A., J. & Elofe. 2002. Information security culture. In *Security in the information society* (pp. 203-214). Boston, MA.: Springer.
- _____, N., & A. da Veiga. 2015. An Information Security Culture Model Validated with Structural Equation Modelling. In *HAI/SA* (pp. 11-21).
- Masrek, M. N., Q. N. Harun, & M. K. Zaini. 2018. The development of an information security culture scale for the Malaysian public organization. *International Journal of Mechanical Engineering and Technology* 9 (7): 1255-1267.
- Mcllwraith, A. 2006. Information security and employee behaviour: How to reduce risk through employee education, training and awareness. Burlington: Gower Publishing Company, Hampshire.
- Moher, D., A. Liberati, J. Tetzlaff, and D. G. Altman. 2009, Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of Internal Medicine* 151 (4): 264-269.
- Nasir, A., R. Abdullah, R. A. Arshah, & M. R. Ab Hamid. 2019. A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective* 28 (3): 55-80.
- _____, R. A. Arshah, & M. R. Ab Hamid. 2017. Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework. In *Proceedings of the 2017 International Conference on Information System and Data Mining* (pp. 56-60). ACM

- _____. 2020. Information Security Culture for Guiding Employee's Security Behaviour: A Pilot Study. In *2020 6th International Conference on Information Management (ICIM)* (pp. 205-209). IEEE.
- Nasir, A., M. Rashid, & A. Hamid. 2018. Conceptualizing and validating information security culture as a multidimensional second-order formative construct. In *The Thirteenth International Multi-Conference on Computing in the Global Information Technology* (pp. 1-8). Venice, Italy.
- Nel, F., & L. Drevin. 2019. Key elements of an information security culture in organisations. *Information & Computer Security* 27 (2):146-164.
- Ngo, L., W. Zhou, & M. Warren. 2005. Understanding transition towards information security culture change. In *Proceedings of 3rd Australian Information Security Management Conference* (pp. 67-73).
- Rotvold, G. 2008. How to create a security culture in your organization? *The Information Management Journal* 1 (4): 33–38.
- Ruhwanya, Z., & J. Ophoff. 2019. Information security culture assessment of small and medium-sized enterprises in Tanzania. In *International Conference on Social Implications of Computers in Developing Countries* (pp. 776-788). Springer, Cham.
- Ruighaver, A. B., S. B. Maynard, & S. Chang. 2007. Organisational security culture: Extending the end-user perspective. *Computers & security* 26 (1): 56-62.
- Sas, M., W. Hardyns, K. van Nunen, G. Reniers, & K. Ponnet. 2021. Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal* 34 (2): 340-357.
- Schlienger, T., & S. Teufel. 2003 September). Analyzing information security culture: increased trust by an appropriate information security culture. In *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.* (pp. 405-409). IEEE.
- Silva, M. 2015. A systematic review of Foresight in Project Management literature. *Procedia Computer Science* 64: 792-799.
- Shahri, A. B., Z. Ismail, & N. Z. A. Rahim. 2013. Security culture and security awareness as the basic factors for security effectiveness in health information systems. *Sains Humanika* 64 (2): 7-12.
- Sherif, E, & S. Furnell. 2015. A conceptual model for cultivating an information security culture. *Int J Inf Security Res* 5 (2): 565–573.
- Shkarlet, S., V. Lytvynov, M. Dorosh, E. Trunova, and M. Voitsekhovska. 2020. The model of information security culture level estimation of organization. *Advances in Intelligent Systems and Computing* 1019: 249-258.
- Solomon, G. and I. Brown. 2020. The influence of organisational culture and information security culture on employee compliance behavior. *Journal of Enterprise Information Management* 34 (4): 1203-1228.
- Tang, M., M. G. Li, & T. Zhang. 2016. The impacts of organizational culture on information security culture: a case study. *Information Technology and Management* 17 (2): 179-186.
- Tolah, A., S. M. Furnell, & M. Papadaki. 2019. A comprehensive framework for understanding security culture in organizations. In *IFIP World Conference on Information Security Education* (pp. 143-156). Springer, Cham.
- _____. 2021. An empirical analysis of the information security culture key factors framework. *Computers & Security* 108: 102354.
- Van Niekerk, J., & R. Von Solms. 2006. Understanding Information Security Culture: A Conceptual Framework. In *ISSA* (pp. 1-10).
2010. _____. Information security culture: A management perspective. *Computers and Security* 29:(4) .476-486
- Von Solms, B. 2000. Information security—The third wave? *Computers & Security* 19 (7): 615–620.

سهیلا جعفر نژاد ثانی

دانشجوی دکتری در رشته مدیریت فناوری اطلاعات از دانشگاه علامه طباطبایی است.

مدیریت فرایندهای کسب و کار، مدیریت خدمات فناوری اطلاعات و سیستم‌های اطلاعاتی مدیریت از جمله علایق پژوهشی وی است.



محمد رضا تقوا

دارای مدرک تحصیلی دکتری در رشته مدیریت توسعه سیستم‌ها از دانشگاه رن فرانسه است. ایشان هم‌اکنون استاد گروه مدیریت صنعتی دانشگاه علامه طباطبایی است.

سیستم‌های اطلاعات مدیریت پیشرفته، هوشمندی کسب و کار، مدیریت خدمات IT و برنامه‌ریزی منابع سازمانی از جمله علایق پژوهشی وی است.



محمد تقی تقوی فرد

دارای مدرک تحصیلی دکتری در رشته مهندسی صنایع از دانشگاه کانزاس آمریکا است. ایشان هم‌اکنون استاد گروه مدیریت صنعتی دانشگاه علامه طباطبایی است.

مدیریت دانش، سرمایه‌گذاری در IT، بهینه‌سازی سیستم‌ها و مدیریت فرایندهای کسب و کار از جمله علایق پژوهشی وی است.



میر علی سیدنقوی

دارای مدرک تحصیلی دکتری در رشته مدیریت دولتی است. ایشان هم‌اکنون استاد گروه مدیریت صنعتی دانشگاه علامه طباطبایی است.

مدیریت منابع انسانی، آموزش و توسعه و مدیریت تحول از جمله علایق پژوهشی وی است.



پژوهش نامه
پژدازش و
مدیریت
اطلاعات

پژوهشگاه علوم انسانی و مطالعات فرهنگی
رتال جامع علوم انسانی