Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

Identifying the Human-Nonhuman Components of Information Security Culture: A Qualitative Study Based on Actor-Network Theory (ANT)

Mohammad Hossein Marzban[1] | **Rahman Sharifzadeh** [2]✉ | **Alireza Poorebrahimi**[3]

1. Ph.D candidate, Department of Information Technology Management, Science and Research Branch, Islamic Azad University, Tehran, Iran, **E-mail:** mo.marzban@iau.ac.ir.
2. Assistant Professor, Iranian Research Institute for Information Sceince snd Technology (IranDoc), Tehran, Iran. **E-mail:** sharifzadeh@irandoc.ac.ir
3. Assistant Professor, Department of Industrial Management, Karaj Branch, Islamic Azad University, Karaj, Iran. **E-mail:** poorebrahimi@gmail.com

Article Info

Article type:
Research Article

Article history:
Received 27 April 2025
Received in revised form 29 May 2025
Accepted 29August 2025
Published online 11 September 2025

Keywords:
Information security culture,
actor-network theory (ANT),
human actor,
non-human actor,
cybersecurity.

ABSTRACT

Purpose: As information becomes one of the most important resources for companies and cyber threats get more advanced, there has been a big increase in spending on security tools. But research shows that over 90% of big security problems come from mistakes made by human. This shows that it's really important to focus on "information security culture" along with technical tools. Most traditional ideas about security culture, like those from Schein and Hofstede, are centered around human and don't take into account the role of non-human elements. This gap in understanding means we need better ways, like Actor-Network Theory, to look at how all different factors work together. This study was done to fill that gap and look at what influences security culture in a major financial organization.

Methodology: The research used a qualitative method and included interviews with 25 managers, experts, and users at the Central Bank of Iran, as well as field observations and document analysis.

Findings: The results showed that security culture comes from the interaction of three main human groups: senior managers who make big decisions, employees who carry out daily tasks, and technical teams that turn policies into real actions. Also, five types of non-human elements were found: policies like ISO 27001, technologies such as SIEM and MFA, physical infrastructure, documents, and organizational processes. A key finding was the role of hybrid actors, like authentication systems, which mix humans and technology and affect how people behave.

Conclusion: Compared to simple models, this study shows that building a better security culture needs a network approach that considers all the different factors. Recommendations include making security tools easier to use, training managers, and embedding security into everyday work. This approach can help financial and governance organizations that face similar challenges.

Cite this article: Marzban, Mohammad Hossein., Sharifzadeh, Rahman., & Poorebrahimi, Alireza. (2025). Identifying the Human-Nonhuman Components of Information Security Culture: A Qualitative Study Based on Actor-Network Theory (ANT). *Human-Information Interaction*, 12(2),46-70.

Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/
Human-Information INTERACTION

Extended Abstract

Introduction

This study tries to find out the human and non-human things that affect how information security culture is formed. It uses the Actor-Network Theory (ANT) to look at this. Today, information is very important for businesses, and there are more cyber threats than ever. Because of this, organizations are spending a lot on security tools. But more than 90% of big security problems come from human errors. This shows that having a strong information security culture is very important, and it works well with technical tools.

Most of the traditional ways of looking at information security culture, like the ones from Schein and Hofstede, focus mainly on people and don't consider non-human factors like technology, rules, or systems. This is a gap in the theory, so using a more complete framework like ANT helps understand how all these factors work together.

ANT looks at how humans and non-humans, such as technology, policies, and infrastructure, are treated equally in networks. It also looks at how ideas and actions change as they move through these networks. This helps understand how information security culture develops over time. The main questions this study looks at are:

What are the important human factors that help create information security culture?

What are the important non-human factors?

What role do hybrid actors—those that mix humans and technology—play in building security culture?

This research is new in theory, method, and practice. It gives a more full picture of how information security culture works by bringing together different kinds of factors.

Methods and Materoal

This study used a qualitative method based on the interpretivist viewpoint. In this approach, there isn’t one true reality—instead, reality is shaped by people’s experiences and how they see things, and it changes depending on the situation. The researcher isn’t just watching from the side; they help build understanding together with the people involved.

The research focused on the Central Bank of the Islamic Republic of Iran because it was seen as the best place to study information security culture. This is because this organisation plays a key role in setting cybersecurity rules for the banking system, faces many complex security threats, and handles highly sensitive financial information. Within this organization, the ongoing balance between strong security policies and the need for new technology created a good setting to look at how people and technology work together.

Data for this study was gathered using semi-structured interviews with 25 managers, experts, and important users. These people were chosen through purposive and snowball sampling until no new ideas were coming up. They were picked because they had at least five years of work experience and were directly involved with security matters in big projects within the organization. The interview questions were based on five main topics, looking through the idea of actor-network theory. These topics covered roles, how people

Journal of Human-Information Interaction
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

interact with technology, things that influence the culture, current problems, and how policies and technology affect how employees behave.

To make the data more complete and credible, we also observed employees' actual behavior on the job and studied documents like security policies, internal reports, and guidelines. Using multiple sources of data in this way helped compare information and cut down on possible biases. The data was analyzed in six steps using the Brown and Clarke content analysis method and the MAXQDA version 2024 software. To make sure the results were accurate and reliable, we also used the participant review technique. The study followed ethical guidelines, including getting informed consent and keeping participants' information private.

Results and Discussion

This study shows that information security culture comes from the ongoing interaction between people and other factors. Among the people involved, three main groups were found: senior managers, who make important decisions, set standards, and allocate resources; regular employees, who carry out daily tasks and are the first line of defense in security, and whose responsibility and quick reporting affect how well security policies work; and technical teams, who help turn policies into action, handle security problems, and provide ongoing training to users.

Among the human challenges, there were several key issues like the mismatch between security rules and how work is done, high work pressure, people not wanting to change their habits, and the balance between user comfort and system security. Also, psychological factors such as the need for trust, being open and honest, and having a personal drive to do the right thing were important in building a security culture. These learning and culture-building efforts were supported by ongoing training, encouraging people to report problems without fear of being punished, and sharing responsibility as a team.

In the section about non-human actors, five main groups were found: policies and standards like ISO 27001 that set rules and guidelines; security tools such as SIEM, DLP, and multi-factor authentication that help watch over systems and influence how people behave; technical systems like networks and hardware; written guides and rules that explain how humans and technology work together; and organizational steps like reporting and feedback processes.

A major part of this study found that there are hybrid actors that exist between humans and non-human elements. These actors include things like multi-factor authentication systems that slowly become part of how people work; policies that use technology to control actions, like automatic limits on copying data; and processes within organizations that help learn about security, such as using attack simulation tools. These hybrid actors show that the line between people and technology in information security culture is not fixed. To improve security culture, it's important to focus on both human and technological aspects at the same time.

When we compare these findings to traditional models, we see that traditional models are mostly focused on humans and see technology as just a tool. However, the actor-network approach treats both humans and non-humans as equal parts of a network. This gives a more connected and changing view of information security culture. In this view, culture isn't something fixed—it comes from the ongoing interactions and discussions between all the different actors involved.

Journal of Human-Information Interaction
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

Conclusion

This study finds that information security culture is formed by the dynamic interaction of human and non-human actors.

Key Human Actors:

- Senior Managers: Make decisions and allocate resources.
- Employees: The first line of defense; their responsibility and reporting are crucial.
- Technical Teams: Implement policies and provide training.

Key Non-Human Actors:

- Policies and standards (e.g., ISO 27001).
- Security tools (e.g., SIEM, DLP, multi-factor authentication).
- Technical infrastructure and written guides.

Crucial Finding: Hybrid Actors

The study highlights "hybrid actors" that blur the line between people and technology, such as:

- Multi-factor authentication becoming a routine part of work.
- Automated policies that enforce rules.
- Attack simulation tools used for training.

So, unlike traditional human-focused models, this study uses an actor-network approach, treating humans and non-humans as equal partners. In this view, security culture is not fixed but is constantly created through the interactions between all these actors. Therefore, improving it requires addressing both human and technological aspects simultaneously.

Keywords: Information security culture, actor-network theory (ANT), human actor, non-human actor, cybersecurity.

نشریه تعامل انسان و اطلاعات
https://hihhu.ac.ir/
شاپا الکترونیکی ۲۴۲۳-۷۴۱۸
دانشگاه خوارزمی

شناسایی مؤلفه‌های انسانی-غیرانسانی فرهنگ امنیت اطلاعات: یک مطالعه کیفی مبتنی بر نظریه کنشگر-شبکه (ANT)

محمدحسین مرزبان[۱]، رحمان شریف‌زاده[۲]✉، علیرضا پورابراهیمی[۳]

۱. دانشجوی دکتری رشته مدیریت فناوری اطلاعات، گروه مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: mo.marzban@iau.ac.ir

۲. نویسنده مسئول، استادیار پژوهشگاه علوم و فناوری اطلاعات ایران (ایران‌داک)، تهران، ایران. رایانامه: sharifzadeh@irandoc.ac.ir

۳. استادیار گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران. رایانامه: poorebrahimi@gmail.com

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخ دریافت:
۱۴۰۴/۰۲/۰۷

تاریخ بازنگری:
۱۴۰۴/۰۳/۰۸

تاریخ پذیرش:
۱۴۰۴/۰۶/۰۷

تاریخ انتشار:
۱۴۰۴/۰۶/۲۰

کلیدواژه‌ها:
فرهنگ امنیت اطلاعات،
نظریه کنشگر-شبکه (انت)،
کنشگر انسانی،
کنشگر غیرانسانی،
امنیت سایبری.

چکیده

هدف: با تبدیل‌شدن اطلاعات به ارزشمندترین دارایی سازمان‌ها و افزایش پیچیدگی تهدیدات سایبری، سرمایه‌گذاری کلانی بر راهکارهای امنیتی صورت گرفته است. بااین‌حال، شواهد نشان می‌دهد که بیش از ۹۰ درصد نقض‌های امنیتی عمده ریشه در خطاهای انسانی دارد. این امر، اهمیت پرداختن به «فرهنگ امنیت اطلاعات» را به‌عنوان مکمل ضروری راهکارهای فنی، بیش‌ازپیش آشکار می‌سازد. مدل‌های سنتی فرهنگ امنیت اطلاعات (مانند مدل‌های شاین و هافستد) عمدتاً انسان‌محور بوده و نقش کنشگران غیرانسانی را نادیده می‌گیرند. این شکاف نظری، ضرورت به‌کارگیری چارچوب‌های جامعی مانند نظریه کنشگر-شبکه (ANT) را برای درک تعامل پویای تمامی عوامل مؤثر ایجاب می‌کند. این مطالعه باهدف پرکردن این شکاف و شناسایی مؤلفه‌های انسانی و غیرانسانی مؤثر در فرهنگ امنیت اطلاعات در یک سازمان مالی حیاتی انجام شد.

روش پژوهش: پژوهش حاضر به روش کیفی تفسیرگرایانه و با تحلیل مصاحبه‌های نیمه‌ساختاریافته با ۲۵ مدیر، کارشناس و کاربر در بانک مرکزی ایران، همراه با مشاهده میدانی و بررسی اسناد انجام شد.

یافته‌ها: نتایج نشان داد فرهنگ امنیتی حاصل تعامل پویای سه گروه انسانی است: ۱)مدیران ارشد (تصمیم‌گیران راهبردی)، ۲)کارکنان (اجراکنندگان رفتارهای روزمره) و ۳)تیم‌های فنی (ترجمه‌کنندگان سیاست‌ها به اقدامات عملی). همچنین، پنج دسته کنشگر غیرانسانی شناسایی شد: سیاست‌ها (مثل ISO 27001)، فناوری‌ها (نظیر SIEM و MFA)، زیرساخت‌ها، اسناد و فرآیندهای سازمانی. نکته کلیدی، نقش کنشگران هیبریدی (ترکیب انسان-فناوری) مانند سیستم‌های احراز هویت بود که رفتار کاربران را تغییر می‌دهند.

نتیجه‌گیری: در مقایسه با مدل‌های خطی، این پژوهش ثابت کرد بهبود فرهنگ امنیتی نیازمند طراحی شبکه‌ای است که تعامل متقابل تمام کنشگران را مدنظر قرار دهد. پیشنهادها شامل توسعه فناوری‌های کاربرپسند، الگوسازی مدیران، و ادغام امنیت در فرآیندهای کاری است. این چارچوب برای سازمان‌های مالی و حاکمیتی که با چالش‌های مشابه روبرو هستند، کاربرد دارد.

استناد: مرزبان، محمدحسین؛ شریف‌زاده، رحمان؛ و پورابراهیمی، علیرضا (۱۴۰۴). شناسایی مؤلفه‌های انسانی-غیرانسانی فرهنگ امنیت اطلاعات: یک مطالعه کیفی مبتنی بر نظریه کنشگر-شبکه (ANT). *تعامل انسان و اطلاعات*، ۱۲(۲)، ۴۶-۷۰.

ناشر: دانشگاه خوارزمی تهران.

مقدمه

امروزه در عصر دیجیتال، اطلاعات به‌عنوان یکی از ارزشمندترین دارایی‌های سازمان‌ها شناخته می‌شود. با افزایش پیچیدگی تهدیدات سایبری و رشد روزافزون حملات سایبری پیچیده، سازمان‌ها در سراسر جهان سالانه میلیاردها دلار صرف راهکارهای امنیتی می‌کنند (سافیترا[1] و همکاران، ۲۰۲۳). بااین‌وجود، گزارش‌های اخیر نشان می‌دهد که بیش از ۹۰٪ نقض‌های امنیتی عمده، ریشه در خطاهای انسانی دارند (نوبلز[2]، ۲۰۲۲). این آمار تکان‌دهنده، اهمیت حیاتی «فرهنگ امنیت اطلاعات» را در کنار راهکارهای فنی برجسته می‌سازد.

فرهنگ امنیت اطلاعات مجموعه‌ای از ارزش‌ها، رفتارها، نگرش‌ها و شیوه‌های مشترک در یک سازمان است که رویکرد کارکنان را برای محافظت از اطلاعات و دستگاه‌های دیجیتال هدایت می‌کند (ویگا[3] و همکاران، ۲۰۲۰؛ تجی[4] و محمد، ۲۰۲۳). این مفهوم چندبعدی شامل مؤلفه‌های مختلفی می‌شود که محققان مختلف آن‌ها را دسته‌بندی کرده‌اند. بر اساس مدل مشهور ادگار شاین[5]، فرهنگ امنیت اطلاعات را می‌توان در سه لایه تعریف کرد. شاین در کتاب «فرهنگ‌سازمانی و رهبری[6]» (۲۰۱۰) فرهنگ‌سازمانی را به‌عنوان الگویی از مفروضات اساسی توصیف می‌کند که گروهی برای حل مشکلات خود ایجاد می‌کند. برای حوزه امنیت اطلاعات، این مدل به‌صورت زیر تطبیق داده می‌شود:

۱. مصنوعات[7]: عناصر قابل‌مشاهده و ملموس مانند رفتارها، سیاست‌ها، ابزارها، محیط فیزیکی؛
۲. ارزش‌های اعلام‌شده[8]: هنجارها و استانداردهای رسمی که سازمان تبلیغ می‌کند و
۳. مفروضات بنیادی[9]: باورهای ناخودآگاه و عمیق‌ترین لایه فرهنگ که رفتارها را هدایت می‌کند.

یا مارتینز و ویگا[10] (۲۰۱۵) مدلی با چهار سازوکار کلیدی توسعه دادند: مدیریت، سیاست‌ها، آگاهی و انطباق، که از طریق مدل‌سازی معادلات ساختاری اعتبارسنجی شد. از سوی دیگر، مدل شلینگر و تویفل[11] (۲۰۰۳) بر سه رکن اساسی تأکید دارد: دانش، نگرش و رفتار. باوجود پیشرفت‌های نظری در حوزه فرهنگ امنیت اطلاعات، رویکردهای موجود از چند جهت دچار محدودیت‌های اساسی هستند. اولاً، این مدل‌ها عمدتاً انسان‌محور بوده و نقش عوامل غیرانسانی را نادیده می‌گیرند. ثانیاً، به تعامل پویا بین عوامل انسانی و غیرانسانی توجه کافی نمی‌کنند. ثالثاً، ماهیت پویا و سیال فرهنگ امنیت اطلاعات را در نظر نمی‌گیرند. این محدودیت‌ها باعث شده است مدل‌های موجود نتوانند به‌خوبی پیچیدگی‌های فرهنگ امنیت اطلاعات در سازمان‌های امروزی را تبیین کنند.

نظریه کنشگر-شبکه (انت) که در دهه ۱۹۸۰ توسط محققانی مانند برونو لاتور، میشل کالون و جان لا توسعه یافت (کالون و لاتور[12]، ۱۹۸۱؛ لاتور، ۱۹۹۶؛ لا[13]، ۲۰۰۸) چارچوبی نوین برای تحلیل پدیده‌های اجتماعی-فنی ارائه می‌دهد. این این نظریه رویکردی متعادل برای درک تعامل بین جنبه‌های اجتماعی و فنی بدون ترجیح یکی بر دیگری ارائه می‌دهد

[1] Safitra
[2] Nobles
[3] Veiga
[4] Tejay & Mohammed
[5] Edgar Schein
[6] Organizational Culture and Leadership
[7] Artifacts
[8] Espoused Values
[9] Basic Underlying Assumptions
[10] Martins & Veiga
[11] Schlienger & Teufel
[12] Callon & Latour
[13] law

(تاتنال[14]، ۲۰۱۲). این نظریه بر دو اصل اساسی استوار است: تقارن بنیادی (نقش متقارن و هم‌اندازه بین انسان‌ها و غیر انسان‌ها و عدم تفاوت و سلسله‌مراتب بین آن‌ها) و فرآیند ترجمه (چگونگی تشکیل شبکه‌های پایدار). انت، هم انسان و هم غیرانسان، نظیر سیستم‌ها و ساختارهای اطلاعاتی را، بازیگر محسوب می‌کند. درواقع انت بر به هم‌پیوستگی بازیگران تأکید کرده و تأکید می‌کند که کنش، شامل افراد و چیزهای زیادی است و دیدگاه‌های سنتی در مورد عاملیت و شروع کنش را به چالش می‌کشد (بنچرکی[15]، ۲۰۱۷). نظریه انت با تأکید بر پیوستگی انسان‌ها و غیر انسان‌ها در شکل دادن به سیستم‌ها و پاسخ‌های امنیتی، دیدگاه منحصربه‌فردی را در مورد امنیت اطلاعات ارائه می‌دهد (سریرماگیری[16] و همکاران، ۲۰۲۲؛ اسکندروف و پاوتوف[17]، ۲۰۲۰؛ لوکسی[18]، ۲۰۲۳). لذا استفاده از انت در مطالعه فرهنگ امنیت اطلاعات چند مزیت کلیدی دارد. اولاً، این نظریه امکان تحلیل جامع‌تری از تمامی عوامل مؤثر را فراهم می‌کند (های[19]، ۲۰۲۵). ثانیاً، به محققان کمک می‌کند تا درک بهتری از تعاملات پیچیده بین عوامل مختلف داشته باشند (هاشمیان و انواری، ۱۳۹۷). ثالثاً، این چارچوب برای مطالعه پویایی‌های فرهنگی در طول زمان مناسب است (جیلانی[20]، ۲۰۲۱). مطالعات معدودی که از انت در حوزه امنیت اطلاعات استفاده کرده‌اند، نشان داده‌اند که این نظریه می‌تواند بینش‌های ارزشمندی ارائه دهد (هایزن و ون د کرک[21]، ۲۰۲۱).

هدف اصلی این مطالعه، شناسایی مؤلفه‌های انسانی-غیرانسانی فرهنگ امنیت اطلاعات بر اساس نظریه کنشگر-شبکه هست. سؤالات اصلی تحقیق عبارت‌اند از:

۱. مؤلفه‌های انسانی مؤثر در شکل‌گیری فرهنگ امنیت اطلاعات کدام‌اند؟

۲. مؤلفه‌های غیرانسانی مؤثر در شکل‌گیری فرهنگ امنیت اطلاعات کدام‌اند؟

۳. کنشگران هیبریدی (ترکیب انسان-فناوری) چه نقشی در شکل‌دهی به فرهنگ امنیتی دارند؟

این تحقیق از چند جهت نوآورانه است. این نوآوری در سه سطح نظری، روش‌شناختی و عملیاتی متجلی شده است: در سطح نظری، با عبور از مدل‌های انسان‌محور صرف، برای نخستین بار «عاملیت» کنشگران غیرانسانی (از فناوری‌هایی مانند SIEM و MFA تا سیاست‌های مکتوب و زیرساخت‌های فیزیکی) در شکل‌دهی، تثبیت و یا حتی تضعیف فرهنگ امنیت اطلاعات به رسمیت شناخته‌شده است. در سطح روش‌شناختی، با به‌کارگیری چارچوب تحلیل مضمون در کنار لنز نظری انت، روشی ترکیبی برای ردیابی و ترسیم شبکه‌های پیچیده کنشگران انسانی و غیرانسانی و تعاملات بین آن‌ها ارائه گردیده است. درنهایت، در سطح عملیاتی، یافته‌های این مطالعه به طراحی یک چارچوب ارزیابی نوین منجر شده که قادر است با نگاهی همه‌جانبه و متقارن، نقاط قوت و ضعف فرهنگ امنیتی سازمان را در تعامل بین انسان و فناوری شناسایی کند و راهکارهایی مبتنی بر «مهندسی مجدد شبکه کنشگران» را به‌جای توصیه‌های صرفاً آموزشی یا فنی پیشنهاد نماید.

مقاله حاضر در هفت بخش سازمان‌دهی شده است. پس‌ازاین مقدمه، بخش دوم به‌مرور ادبیات می‌پردازد. بخش سوم روش تحقیق را شرح می‌دهد. بخش چهارم یافته‌ها را ارائه می‌کند. بخش پنجم به بحث و تحلیل یافته‌ها اختصاص دارد.

[14] Tatnall
[15] Bencherki
[16] Sreeramagiri
[17] Iskanderov & Pautov
[18] Luxi
[19] Hay
[20] Jelani
[21] Van de Kerke & Hijzen

بخش ششم نتیجه‌گیری و پیشنهادها را ارائه می‌دهد.

یافته‌های این تحقیق می‌تواند به سازمان‌ها در طراحی راهکارهای مؤثرتر برای بهبود فرهنگ امنیت اطلاعات کمک کند. همچنین می‌تواند مبنایی برای توسعه ابزارهای ارزیابی فرهنگ امنیت اطلاعات قرار گیرد. از دیدگاه نظری، این مطالعه به غنای ادبیات حوزه امنیت اطلاعات و نظریه کنشگر-شبکه می‌افزاید.

پیشینه پژوهش

(مارتینز و الوف[۲۲]، ۲۰۰۲) فرهنگ امنیت اطلاعات را به‌عنوان «فرضی درباره ادراکات و نگرش‌هایی می‌داند که به‌منظور ترکیب ویژگی‌های امنیت اطلاعات به‌عنوان روشی که در آن کارها در یک سازمان انجام می‌شود، باهدف حفاظت از دارایی‌های اطلاعاتی پذیرفته‌شده است» که بیشتر به نقشی که رفتار کارکنان در حفاظت از داده‌ها ایفا می‌کند اشاره دارد. فرهنگ که ارزش‌ها، باورها و رفتارهای یک گروه را در برمی‌گیرد، تأثیر قابل‌توجهی بر رویه‌های امنیت اطلاعات و انطباق در سازمان‌ها دارد (هنگستلرو پریاژنیکووا[۲۳]، ۲۰۲۱). سازمان‌هایی که فرهنگ امنیتی قوی دارند، آسیب‌پذیری سایبری مبتنی بر انسان کمتری دارند (پارسونز[۲۴] و همکاران، ۲۰۱۵). بااین‌حال، ایجاد یک فرهنگ امنیت اطلاعات، چالش‌برانگیز است و نیازمند یک رویکرد سیستماتیک و چند رشته‌ای است (هنگستلر و پریاژنیکوا، ۲۰۲۱). عواملی مانند ارزش‌های فرهنگی فردی و فرهنگ‌سازمانی غالب باید هنگام توسعه استراتژی‌های امنیتی در نظر گرفته شوند (سالامن و براون[۲۵]، ۲۰۲۰؛ تانگ[۲۶] و همکاران، ۲۰۱۶). لذا فرهنگ امنیت اطلاعات، به‌عنوان بخشی جدایی‌ناپذیر از فرهنگ‌سازمانی، برای دفاع سایبری حیاتی است و بر رفتار امنیتی کارکنان تأثیر می‌گذارد (کانلانگینگ و کاتسیکاس[۲۷]، ۲۰۲۳؛ داویگا[۲۸] و همکاران، ۲۰۲۰؛ اوچندو[۲۹] و همکاران، ۲۰۲۱؛ اوگبانوفه[۳۰]، ۲۰۲۱).

همان‌طور که می‌دانیم، امنیت سایبری و امنیت اطلاعات یک سازمان در یک فضای ترکیبی از فنّاوری‌ها و کاربر نهایی قرار دارد و هم کاربران و هم فناوری در تهدیدات و بالطبع امنیت سازمان نقش داشته و در تعامل با یکدیگر بوده و بر هم اثر می‌گذارند (اصلان و همکاران[۳۱]، ۲۰۲۳). درواقع یکی از مسائل اصلی که در حوزه امنیت سایبری وجود دارد، عدم وجود دیدگاهی متقارن و متعادل در میزان اهمیت و تمرکز بین مسائل فنی و تکنولوژیکی و انسان و مسائل اجتماعی و ویژگی‌های فردی است (دی آزمبوجا[۳۲] و همکاران، ۲۰۲۳).

مفهوم فرهنگ امنیت اطلاعات از جنبه‌های مختلفی در تحقیقات علمی موردبررسی قرارگرفته است. مطالعات نشان می‌دهد که این حوزه پژوهشی از تنوع روش‌شناختی برخوردار است، به‌طوری‌که برخی پژوهش‌ها به ارائه چارچوب‌های نظری پرداخته‌اند، درحالی‌که تعدادی دیگر بر جنبه‌های کاربردی و عملیاتی تمرکز کرده‌اند.

[22] Martins & Eloff
[23] Hengstler & Pryazhnykova
[24] Parsons
[25] Solomon & Brown
[26] Tang
[27] Kannelonging & Katsikas
[28] Da Veiga
[29] Uchendu
[30] Ogbanufe
[31] Aslan
[32] De Azambuja

شلینگر و تویفل (۲۰۰۳) از پیشگامان ارائه مدل‌های مفهومی در این حوزه بودند. پس از آن‌ها، چانگ و لین[۳۳] (۲۰۰۷) با طراحی چارچوبی به بررسی رابطه بین فرهنگ‌سازمانی و مدیریت امنیت اطلاعات پرداختند. در همین راستا، النظیر و نلسون[۳۴] (۲۰۰۹) چارچوبی برای درک بهتر فرهنگ امنیت اطلاعات در بسترسازمانی توسعه دادند.

در سطح عملیاتی، دوجکوفسکی و همکاران[۳۵] (۲۰۰۷) راهکارهایی برای پیاده‌سازی فرهنگ امنیت اطلاعات در شرکت‌های کوچک و متوسط ارائه کردند. داویگا و الوف[۳۶] (۲۰۱۰) نیز چارچوبی عملی برای ارزیابی و ارتقای فرهنگ امنیت اطلاعات در سازمان‌ها طراحی نمودند. این مطالعات نشان داد که اجرای موفقیت‌آمیز فرهنگ امنیت اطلاعات به عوامل سازمانی متعددی وابسته است. برخی پژوهش‌ها به بررسی این مفهوم در حوزه‌های خاص پرداخته‌اند. به‌عنوان‌مثال، شهری و همکاران[۳۷] (۲۰۱۳) و حسن و اسماعیل[۳۸] (۲۰۱۲) مدل‌هایی را برای محیط‌های مراقبت سلامت توسعه دادند. این مدل‌ها بر ایجاد امنیت مؤثر در سیستم‌های اطلاعات سلامت تأکید داشتند. پژوهشگرانی مانند چن و همکاران[۳۹] (۲۰۱۵) و الفواز و همکاران[۴۰] (۲۰۱۰) به بررسی تفاوت‌های فرهنگی در پیاده‌سازی امنیت اطلاعات پرداختند. النظیر (۲۰۱۴) نیز ویژگی‌های فرهنگ‌سازمانی مؤثر بر امنیت اطلاعات را در بسترهای فرهنگی مختلف موردمطالعه قرارداد. ساس و همکاران[۴۱] (۲۰۲۱) و شکارلت[۴۲] و همکاران (۲۰۲۰) روش‌های نوینی برای ارزیابی فرهنگ امنیت اطلاعات ارائه کردند. لیم و همکاران[۴۳] (۲۰۱۰) ابزاری طراحی نمودند که به سازمان‌ها کمک می‌کند میزان ادغام فرهنگ امنیت اطلاعات در فرهنگ‌سازمانی خود را بسنجند.

مرور سیستماتیک پژوهش‌های انجام‌شده توسط الهوجیل و میرزا[۴۴] (۲۰۱۵)، کارلسون و همکاران[۴۵] (۲۰۱۵) و داویگا و همکاران (۲۰۲۰) نشان می‌دهد که علی‌رغم گستردگی تحقیقات، هنوز شکاف‌های دانشی قابل‌توجهی در این حوزه وجود دارد. این مطالعات تأکید می‌کنند که بسیاری از پژوهش‌های موجود ماهیتاً نظری هستند و نیاز به تحقیقات تجربی بیشتری احساس می‌شود. همچنین جعفرنژاد ثانی و همکاران (۱۴۰۲) نیز یک مطالعه سیستماتیک و مروری انجام دادند که با بررسی ۳۱۰ مقاله از سال ۲۰۰۰ تا ۲۰۲۲، به تحلیل ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات پرداخته است. یافته‌ها نشان می‌دهند که اجماعی بر سر ابعاد و مؤلفه‌های این فرهنگ وجود ندارد و محققان از نظریه‌های مختلفی مانند مدل فرهنگ‌سازمانی «شاین[۴۶]» استفاده کرده‌اند (شاین، ۱۹۸۳). بیشتر پژوهش‌ها در کشورهای درحال‌توسعه انجام‌شده و مدل‌های پیشنهادی اغلب توصیفی و بدون ارزیابی عملی هستند. همچنین، هیچ چارچوب خاصی برای صنایع مختلف ارائه نشده است.

[33] Chang & Lin
[34] Alnatheer & Nelson
[35] Dojkovski
[36] Da Veiga & Eloff
[37] Shahri
[38] Hassan & Ismail
[39] Chen
[40] Alfawaz
[41] Sas
[42] Shkarlet
[43] Lim
[44] AlHogail & Mirza
[45] Karlsson
[46] Schein

بررسی مطالعات اخیر در حوزه فرهنگ امنیت اطلاعات نشان می‌دهد که این پژوهش‌ها باوجود تنوع روش‌شناختی و جغرافیایی، همگی بر عوامل انسانی و سازمانی به‌عنوان محور اصلی شکل‌گیری فرهنگ امنیتی تأکید کرده‌اند. مطالعاتی مانند تحقیق زانکه و همکاران[۴۷] (۲۰۲۴) بر نقش تعهد مدیریت و برنامه‌های آموزشی، کار میکولتیچ و همکاران[۴۸] (۲۰۲۴) بر ارتباط نگرش کارکنان با رفتارهای امنیتی و پژوهش تجی و محمد (۲۰۲۳) بر تأثیر انسجام گروهی و کدهای حرفه‌ای تمرکز دارند. حتی هنگام بررسی فناوری‌های نوظهور مانند معماری اعتماد صفر (زیود و لطفی[۴۹]، ۲۰۲۴) یا خط‌مشی‌های امنیتی (کارلسون و همکاران، ۲۰۲۲)، تحلیل‌ها صرفاً بر پذیرش انسانی یا انطباق سازمانی متمرکز بوده‌است. این جهت‌گیری مشترک، منجر به غفلت نظام‌مند از نقش کنشگران غیرانسانی در شکل‌دهی به فرهنگ امنیت اطلاعات شده است. فناوری‌ها، زیرساخت‌ها و اسناد خط‌مشی صرفاً به‌عنوان ابزارهای منفعلِ پیاده‌سازی تصمیمات انسانی تصویر شده‌اند، درحالی‌که در واقعیت، این عناصر غیرانسانی به‌طور فعال بر رفتارهای امنیتی تأثیر می‌گذارند. برای مثال، سیستم‌های تشخیص نفوذ خودکار نه‌فقط ابزارهای نظارتی، بلکه بازتعریف‌کننده هنجارهای پذیرفته‌شده امنیتی هستند. مستندات خط‌مشی تنها مجموعه‌ای از دستورالعمل‌ها نیستند، بلکه با ماهیت مادی خود (دسترسی‌پذیری، قالب‌بندی، زبانی که استفاده می‌کنند) مشروعیت اقدامات امنیتی را می‌سازند یا تضعیف می‌کنند. حتی طراحی فیزیکی محیط کار (مانند اتاق‌های سرور شیشه‌ای یا محل‌های نصب دوربین‌ها) پیام‌های ناخودآگاه درباره اولویت‌های امنیتی ارسال می‌کند. این غفلت از کنشگری غیرانسانی، درک ما را از پویایی‌های فرهنگ امنیتی ناقص کرده است.

پیامد این نگاه تک‌بعدی، طراحی مدل‌هایی است که قادر به پیش‌بینی تأثیر تحولات فناورانه (مانند هوش مصنوعی یا اتوماسیون پیشرفته) بر فرهنگ امنیتی نیستند و تاب‌آوری سازمان‌ها را در برابر اختلالات زیرساختی کاهش می‌دهد. برای نمونه، مطالعاتی مانند اورهک و پتریچ[۵۰] (۲۰۲۱) که به ضعف مقیاس‌های سنجش فرهنگ امنیت اطلاعات اعتراف می‌کنند، هرگز این پرسش را مطرح نمی‌سازند که آیا علت اصلی این ضعف، نادیده گرفتن تعامل پویای انسان‌ها با سیستم‌های فنی است؟ بنابراین، ضروری است پژوهش‌های آتی فرهنگ امنیت اطلاعات را نه به‌عنوان محصول انحصاری تصمیمات انسانی، بلکه به‌مثابه پدیده‌ای انسان‌فناورانه بازتعریف کنند که در شبکه‌ای از کنشگران انسانی و غیرانسانی (فناوری‌ها، اسناد، زیرساخت‌ها) شکل می‌گیرد. این تغییر پارادایم مستلزم روش‌شناسی‌هایی است که توانایی ردیابی نحوه تأثیرگذاری متقابل این عناصر بر یکدیگر را داشته باشند. این شکاف پژوهشی نشان‌دهنده نیاز به اتخاذ چارچوب‌های نظری جامع‌تری مانند نظریه کنشگر-شبکه است که بتواند روابط پیچیده بین تمامی عناصر انسانی و غیرانسانی مؤثر بر فرهنگ امنیت اطلاعات را تحلیل کند.

نظریه انت به عنوان چارچوبی ارزشمند برای تحلیل امنیت و فناوری در زمینه‌های مختلف آموزشی و سازمانی ظهور کرده است. انت قدرت را ناشی از پیوندهای وضع‌شده می‌داند نه ساختارهای موجود (بارون و گومز[۵۱]، ۲۰۱۶). این نظریه می‌تواند با بررسی شبکه‌های ناهمگن بازیگران انسانی و غیرانسانی که نشان می‌دهد چگونه نقض‌های امنیتی از طریق ناهماهنگی منافع رخ می‌دهد، برای درک مدیریت امنیت اطلاعات به‌کار گرفته شود (هدستروم و همکاران[۵۲]، ۲۰۱۰). انت همچنین با

[47] Zanke
[48] Mikuletič
[49] Zyoud & Lutfi
[50] Orehek & Petrič
[51] Baron & Gómez
[52] Hedström

تحلیل تعاملات بین فعالیت‌های آگاهی‌بخشی و فرآیندهای سازمانی، بینش‌هایی در مورد چالش‌های اجرای برنامه‌های آگاهی‌بخشی امنیت اطلاعات ارائه می‌دهد (تسوهو[۵۳] و همکاران، ۲۰۱۲). درمجموع، انت دیدگاهی منحصربه‌فرد برای مطالعه روابط پیچیده بین فناوری، امنیت و عوامل اجتماعی در محیط‌های مختلف ارائه می‌دهد.

پژوهش‌های متعددی با تکیه‌بر نظریه کنشگر-شبکه به تحلیل چالش‌ها و راهکارهای امنیت سایبری در سطوح مختلف پرداخته‌اند. اِکه‌گوئی[۵۴] (۲۰۲۳) در مطالعه‌ای با مصاحبه‌های نیمه‌ساختاریافته نشان داد که تهدیداتی مانند تهدیدات داخلی و حملات فیشینگ سازمان‌ها را تحت تأثیر قرار می‌دهند و عواملی مانند چالش‌های رفتاری و محدودیت‌های اجرایی به عدم پایبندی به سیاست‌های امنیتی منجر می‌شوند. این پژوهش تأکید کرد که توسعه اثربخش سیاست‌های امنیت سایبری نیازمند رویکردی مشارکتی با حضور ذینفعان سازمانی است. در سطح کلان‌تر(آلام[۵۵] و همکاران، ۲۰۲۵) با مصاحبه‌های بدون ساختار، مدلی سه‌بخشی برای امنیت سایبری شهرهای هوشمند اندونزی طراحی کرد که شامل: ذینفعان امنیت سایبری، مبانی حقوقی مدیریت امنیت، و سازوکارهای مدیریتی است. این مدل مبتنی بر مراحل ترجمه انت، عوامل کلیدی اجرای امنیت سایبری را شناسایی می‌کند.

سریراماگیری[۵۶] و همکاران (۲۰۲۲) با ردیابی شبکه‌های تولیدی اثبات کردند که حملات سایبری تنها به سیستم‌های فیزیکی محدود نمی‌شوند، بلکه پیامدهایی گسترده مانند خطرات ایمنی فیزیکی، تغییر افکار عمومی و اختلال در بازارهای اقتصادی ایجاد می‌کنند. ادغام انت با تحقیقات تولیدی، درک جامعی از این پیامدها ارائه می‌دهد. در تحلیل قربانیان سایبری، ون در واگن و پیترز[۵۷] (۲۰۲۰) بامطالعه مواردی مانند باج‌افزار و بات‌نت‌ها، قربانی را یک کنشگر-شبکه ترکیبی متشکل از انسان‌ها و فناوری‌ها تعریف کردند. آن‌ها قربانی شدن را نتیجه تعامل پیچیده‌ای بین برنامه‌های کنش (انسانی/غیرانسانی) و ضد برنامه‌ها دانستند. لبافی[۵۸] (۲۰۲۰) نیز در پژوهش خود درباره سیاست حفاظت از داده‌ها در ایران، با مصاحبه ۱۸ بازیگر نشان داد که اجرای موفق سیاست‌ها مستلزم همسویی منافع و مشارکت بازیگران کلیدی در مرحله "بسیج" شبکه است.

پژوهش‌هایی مانند شریف‌زاده (۱۴۰۲) و رستمی و همکاران (۱۴۰۱) چارچوب‌های روش‌شناختی انت را بومی‌سازی کردند. شریف‌زاده با تلفیق نشانه‌شناسی و پدیدارشناسی، یک چارچوب چهارمرحله‌ای برای پژوهش‌های کیفی ارائه داد. رستمی نیز ۵ گام تحلیل مبتنی بر انت را معرفی کرد: ۱. شناسایی موجودیت‌ها ۲. شکل‌گیری موجودیت‌ها ۳. تبدیل موجودیت به کنشگر ۴. پایدارسازی-سازماندهی ۵. ساده‌سازی-کارکردمندسازی. این پژوهش‌ها بر استفاده از معیارهای تکثرگرایی، بازبینی توسط اعضا و ردیابی ممیزی برای تضمین اعتبار نتایج تأکیددارند.

بالزاک و کاولتی[۵۹] (۲۰۱۶) با تحلیل حمله استاکس‌نت نشان دادند بدافزارها با به‌چالش‌کشیدن مرزهای سیال، شبکه‌ها و مناطق حاکمیتی، مداخلات سیاسی را فعال می‌کنند. هدستروم و همکاران (۲۰۱۰) نیز هک در محیط‌های دانشگاهی را نتیجه ناهم‌ترازی منافع در شبکه‌های ناهمگن دانستند و امنیت را محصول ثبات و نظم اجتماعی حاصل از همسویی کنشگران تعریف کردند. اسماعیلی و همکاران (۱۴۰۱) با روش سناریوسازی نشان دادند فناوری بلاک‌چین می‌تواند

[53] Tsohou
[54] Okigui
[55] Alam
[56] Sreeramagiri
[57] Van der Wagen & Pieters
[58] Labafi
[59] Balzacq & Cavelty

مدیریت اطلاعات در سازمان‌هایی مانند تأمین اجتماعی را متحول کند. نازی و همکاران (۱۳۹۹) نیز با ارائه مدلی متقارن، تأکید کردند تعامل با اطلاعات باید هم‌زمان نقش انسان‌ها و عوامل غیرانسانی (مانند زیرساخت‌ها) را در نظر گیرد.

با به‌کارگیری انت در مدیریت امنیت اطلاعات، سازمان‌ها می‌توانند بینش‌هایی را در مورد شبکه پیچیده روابط و وابستگی‌هایی که روی شیوه‌ها و نتایج امنیتی تأثیر می‌گذارند به دست آورند (والشام[۶۰]، ۱۹۹۷). این رویکرد با در نظر گرفتن نه‌تنها کنترل‌های رسمی، بلکه روابط غیررسمی، مانند شبکه‌سازی و مذاکره، که در دستیابی به اهداف امنیتی بسیار مهم هستند، امکان درک جامع‌تری از فرآیندهای امنیتی را فراهم می‌کند (سویرف و سلتسیکاس[۶۱]، ۲۰۱۴).

لذا نظریه کنشگر-شبکه با تمرکز بر شبکه‌های ناهمگن (شامل انسان‌ها، فناوری‌ها، قوانین و سازمان‌ها) نشان می‌دهد امنیت سایبری صرفاً یک مسئله فنی نیست، بلکه محصول تعامل پویای عناصری است که در قالب شبکه‌های پیچیده عمل می‌کنند. این نظریه با آشکارسازی تعارض منافع، چالش‌های اجرایی و پیامدهای غیرمستقیم حملات، چارچوبی تحلیلی برای طراحی سیاست‌های امنیتی جامع و انعطاف‌پذیر فراهم می‌کند.

روش‌شناسی

با توجه به سؤالات و موضوع تحقیق، پارادایم این تحقیق (روش‌شناسی) کیفی و بر اساس فلسفه تحقیق تفسیرگرایی[۶۲] است (گیچورو[۶۳]، ۲۰۱۷). زیرا فرض می‌کنیم که هیچ حقیقت واحدی (هستی‌شناسی) وجود ندارد و حقیقت به‌صورت زمینه‌ای یا ذهنی (معرفت‌شناسی) از طریق ادراکات و تجربیات شرکت‌کنندگان همان‌طور که توسط (کیونجا و کوئینی[۶۴]،۲۰۱۷) بحث شده است، ساخته می‌شود.

این رویکرد، با تأکید بر اینکه همه داده‌ها نیاز به تفسیر دارند و محققان به‌طور فعال در کنار شرکت‌کنندگان به ساخت معانی می‌پردازند، تجربه‌گرایی پوزیتیویستی را به چالش می‌کشد (الهراشه و پیوس[۶۵]، ۲۰۲۰). این رویکرد، شرکت‌کنندگان را به‌عنوان همکارانی در معناسازی می‌بینند، نه سوژه‌هایی که باید کنترل شوند (داربی و همکاران[۶۶]، ۲۰۱۹).

مطالعه حاضر در بانک مرکزی جمهوری اسلامی ایران انجام‌شده است که به‌عنوان بالاترین مرجع تنظیم‌گری نظام بانکی کشور، نقش محوری در طراحی و نظارت بر سیاست‌های امنیت سایبری و فناوری‌های دیجیتال در شبکه بانکی ایفا می‌کند. این سازمان به دلیل مواجهه مستمر با تهدیدات سایبری پیچیده و حساسیت فوق‌العاده داده‌های مالی تحت مدیریتش، به‌عنوان یک محیط پژوهشی ایده‌آل برای بررسی فرهنگ امنیت اطلاعات انتخاب شد. تمرکز اصلی مطالعه بر چند ادارات مختلفی بوده است که با مسائل مختلف حوزه فناوری اطلاعات و ریسک‌های موجود در ارتباط می‌باشند.

در این سازمان، تعاملات پویا و گاه تنش‌آمیز بین الزامات امنیتی سخت‌گیرانه و نیاز به نوآوری‌های فناورانه، بستری غنی برای مشاهده نقش کنشگران انسانی و غیرانسانی در شکل‌دهی به فرهنگ امنیت اطلاعات فراهم کرده است. از یک‌سو، متخصصان امنیت سایبری به‌عنوان کنشگران انسانی کلیدی، مدام در حال مذاکره با مدیران فناوری برای اجرای سیاست‌های امنیتی هستند و از سوی دیگر، سیستم‌های هوشمند تحلیل رفتار مانند پلتفرم تشخیص ناهنجاری‌های

[60] Walsham
[61] Soyref & Seltsikas
[62] Interpretivism
[63] Gichuru
[64] Kivunja & Kuyini
[65] Alharahsheh & Pius
[66] Darby

تراکنشی، به‌عنوان کنشگران غیرانسانی تأثیرگذار، رفتار کارکنان را در مواجهه با داده‌های حساس شکل می‌دهند. این پیچیدگی زمانی آشکارتر می‌شود که اسناد بالادستی مانند: سند راهبردی نظام جامع فناوری اطلاعات ایران، سند راهبرد هوش مصنوعی کشور، سند راهبرد فناوری‌های نوین بانک مرکزی، سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور را به‌عنوان کنشگران غیرانسانی مؤثر در نظر بگیریم که نحوه تعامل انسان و فناوری را در سطح کلان تعیین می‌کنند.

انتخاب این سازمان به‌عنوان زمینه مطالعه، علاوه بر دسترسی پژوهشگر به خبرگان و اسناد تخصصی، به دلایل متعددی صورت گرفته است. نخست آنکه تنوع کنشگران حاضر در این محیط (از مدیران ارشد تنظیم‌گر گرفته تا سیستم‌ها و پروتکل‌ها) امکان بررسی جامع‌تری از پدیده فرهنگ امنیت اطلاعات را فراهم می‌کند. دوم آنکه چالش‌های منحصربه‌فرد این سازمان، مانند نیاز به توازن بین امنیت و کارایی در سامانه‌های پرداخت ملی، نمونه‌ای بارز از تعاملات پیچیده در شبکه‌های کنشگران است. درنهایت، یافته‌های این مطالعه می‌تواند برای سایر نهادهای مالی و حاکمیتی که با مسائل مشابهی روبرو هستند، راهگشا باشد.

مصاحبه‌های این پژوهش با ۲۵ نفر از ذی‌نفعان کلیدی انجام‌شده است. این افراد از میان معاونت‌های نظارت و فناوری‌های نوین بانک مرکزی انتخاب شدند تا طیف کاملی از دیدگاه‌های مرتبط بافرهنگ امنیت اطلاعات را پوشش دهند. مبنای انتخاب مصاحبه‌شوندگان، سابقه کاری حداقل پنج سال در حوزه مربوطه و درگیری مستقیم با مسائل حوزه امنیتی و فناوری اطلاعات در پروژه‌های کلان سازمان بوده است. در این تحقیق از روش نمونه‌گیری هدفمند تا رسیدن به اشباع نظری با حداکثر تنوع و از مصاحبه نیمه ساختاریافته و روش هدفمند گلوله برفی استفاده شد.

در مورد تعداد مصاحبه‌های لازم، تعداد از پیش تعیین‌شده‌ای وجود ندارد و تعیین حجم نمونه کافی در تحقیقات کیفی شامل قضاوت، در نظر گرفتن روش تحقیق، استراتژی نمونه‌گیری و حوزه تحقیقی موردنظر است (ساندلوفسکی[۶۷]، ۱۹۹۵). طبق (کرسول و پوت [۶۸]، ۲۰۱۳؛ گِست[۶۹] و همکاران، ۲۰۰۶)، ۱۲ تا ۳۰ مصاحبه برای اکثر پژوهش‌های کیفی کافی است. در این تحقیق پس از ۲۵ مصاحبه به اشباع کامل رسیده شد. سؤالات مصاحبه از طریق ۵ سؤال با لنز انت طراحی شد:

سؤال ۱: می‌توانید نقش و مسئولیت‌های خود را در رابطه با امنیت اطلاعات در سازمانتان شرح دهید؟

سؤال ۲: چگونه در کارهای روزمره خود با فناوری‌ها یا سیستم‌های امنیت اطلاعات تعامل دارید؟

سؤال ۳: به نظر شما، چه عناصر کلیدی‌ای فرهنگ امنیت اطلاعات در سازمان شما را شکل می‌دهند؟

سؤال ۴: چه چالش‌ها یا موانعی در حفظ یا بهبود امنیت اطلاعات تجربه می‌کنید و چگونه با آن‌ها مقابله می‌کنید؟

سؤال ۵: به نظر شما، فناوری‌ها یا سیاست‌های امنیت اطلاعات در سازمانتان چگونه بر رفتار کارکنان و فرهنگ کلی امنیت تأثیر می‌گذارند؟

این مجموعه سؤالات به‌صورت نظام‌مند طراحی‌شده‌اند تا داده‌های غنی و چندبعدی برای پاسخ به سؤالات اصلی پژوهش فراهم آورند.

در این پژوهش، علاوه بر مصاحبه‌های نیمه‌ساختاریافته با مشارکت‌کنندگان کلیدی، از داده‌های مکمل شامل مشاهده‌های میدانی و تحلیل اسناد و مدارک مرتبط استفاده شد. این رویکرد دوسطحی (مطالعات سندی و مصاحبه) به درک جامع‌تر و اعتباربخشی یافته‌ها کمک کرد. مشاهده‌ها به‌ویژه در بررسی رفتارهای عملی و زیسته مرتبط با امنیت

[67] Sandelowski
[68] Creswell & poth
[69] Guest

اطلاعات و فرآیندهای سازمانی موردتوجه قرار گرفت، درحالی‌که اسناد (مانند خط‌مشی‌های امنیتی، گزارش‌های داخلی و دستورالعمل‌ها) زمینه‌های رسمی و مکتوب فرهنگ امنیت اطلاعات را تکمیل نمود. ترکیب این منابع داده‌ای، امکان تحلیل تطبیقی و کاهش سوگیری‌های احتمالی ناشی از تک‌روشی بودن را فراهم آورد.

جهت تحلیل داده‌های جمع‌آوری‌شده، از چارچوب تحلیل مضمون به روش براون و کلارک[۷۰] (۲۰۰۶، ۲۰۱۴ و ۲۰۲۱) که یکی از پرکاربردترین و تأثیرگذارترین روش‌های تحلیل کیفی محسوب می‌شود، استفاده گردید. این روش تحلیل در ۶ مرحله صورت می‌گیرد. چارچوب تحلیل مضمون براون و کلارک رویکردی قدرتمند، انعطاف‌پذیر و درعین‌حال ساختاریافته برای تحلیل داده‌های کیفی ارائه می‌دهد. برای این کار از نرم‌افزار MAXQDA نسخه ۲۰۲۴ استفاده شد.

اعتباربخشی[۷۱] در تحقیقات کیفی به روش‌های مختلفی انجام می‌شود که ازجمله آن‌ها، مثلث‌سازی[۷۲] و بازبینی مشارکت‌کنندگان[۷۳] می‌باشند. مثلث‌سازی در تحقیقات کیفی، راهبردی است که برای افزایش اعتبار و توسعه درک جامع از پدیده‌ها با به‌کارگیری روش‌ها یا منابع داده چندگانه استفاده می‌شود. چهار نوع مثلث‌بندی شناسایی‌شده‌اند: مثلث‌بندی روش، محقق، نظریه و منبع داده‌ها (کارتر[۷۴]، ۲۰۱۴). مثلث‌بندی‌های چندگانه می‌توانند به‌عنوان یک استراتژی اعتبارسنجی مورداستفاده قرار گیرند و به محققان اجازه دهند رویدادها را از زوایای مختلف بررسی کنند و سوگیری را به حداقل برسانند (سانتوس[۷۵] و همکاران، ۲۰۲۰). با توجه به اینکه ما از دو منبع (افراد و اسناد) و همچنین افراد مختلف در زمان‌ها وادارات متفاوت جهت جمع‌آوری داده‌ها استفاده می‌کنیم، لذا از روش مثلث‌بندی منابع داده بهره برده شده است.

مضافاً ما از تکنیک بازبینی مشارکت‌کنندگان نیز استفاده کرده‌ایم که در تحقیقات کیفی برای افزایش اعتبار با اجازه دادن به شرکت‌کنندگان برای بررسی و اعتبارسنجی داده‌ها یا نتایج استفاده می‌شود (بیرت[۷۶] و همکاران، ۲۰۱۶). این تکنیک، می‌تواند در اعتبارسنجی یافته‌ها، آشکار کردن اطلاعات جدید و مشاهده واگرایی بین گروه‌های شرکت‌کننده مؤثر باشد (سانتوس و همکاران، ۲۰۱۷).

لازم به ذکر است پژوهش حاضر با رعایت اصول اخلاقی رضایت آگاهانه و محرمانگی انجام‌شده است تا علاوه بر تولید دانش معتبر، احترام به حقوق انسانی مشارکت‌کنندگان نیز تضمین گردد.

یافته‌ها

مؤلفه‌های انسانی در جدول (۱) نشان داده‌شده است:

جدول (۱): مؤلفه‌های انسانی مؤثر در فرهنگ امنیت اطلاعات بر اساس نظریه انت

رده اصلی	زیررده	یافته‌های کلیدی
کنشگران انسانی	رفتارهای انسانی	-گزارش‌دهی سریع مشکلات توسط کاربران (فرم‌های بازخورد). -مسئولیت‌پذیری فردی (عاملیت توزیع‌شده) -واکنش به تهدیدات نوظهور (محدودسازی دسترسی، تنظیمات فایروال، برگزاری جلسات توجیهی و مشارکت دادن ذی‌نفعان، شرکت در نشست‌ها و ارتباط با دانشگاه‌ها، شرکت در همایش‌های بین‌المللی). -اشکال‌زدایی پس از به‌روزرسانی‌ها.

[70] Braun & Clarke
[71] Validation
[72] Triangulation
[73] Member Checking
[74] Carter
[75] Santos
[76] Birt

	مدیران-کنشگران کلیدی	-تدوین سیاست‌های امنیتی متناسب با استانداردهای بین‌المللی. -فرهنگ‌سازی امنیتی از طریق الگوسازی مدیران. -هماهنگی استراتژیک برای مقابله با تهدیدات. -تعادل بین امنیت و کارایی عملیاتی.
	کاربران فنی-کنشگران واسط	-شناسایی آسیب‌پذیری‌ها توسط کارشناسان امنیت. -بررسی پروژه‌های جدید توسط ناظران امنیت اطلاعات. -فرهنگ‌سازی امنیتی از طریق آموزش کاربران. -نقش واسطه‌گر شبکه امنیتی بین تیم‌های فنی و مدیریتی.
	کارکنان عادی	-مقاومت در برابر تغییرات امنیتی (مثل MFA) -نقش "نگهبان روزمره" امنیت اطلاعات. -گزارش‌دهی مشکلات توسط کاربران ساده. -عاملیت توزیع‌شده (امنیت به‌عنوان یک زنجیره).
چالش‌های انسانی	چالش‌های اجرایی	-ناهماهنگی بین سیاست‌های امنیتی و روندهای کاری. -فشار کاری و تنگنای زمانی. -مقاومت کارکنان در برابر تغییرات. -تداخل بین راحتی کاربر و امنیت سیستم.
	فرهنگی/روانی	-مقاومت فرهنگی در برابر سیاست‌های جدید. -ترس از تنبیه و عواقب اشتباهات. -احساس محدودیت و کنترل بیش‌ازحد. - نیاز به شفافیت و توضیح منطقی سیاست‌ها.
عوامل روان‌شناختی	اعتماد/عدم اعتماد	-اهمیت شفافیت در سیاست‌ها برای جلب اعتماد. -احساس امنیت بیشتر با گزارش‌دهی بدون تنبیه. -تأثیر مثبت تشویق و بازخورد مثبت.
	انگیزش درونی	-نقش خلاقیت در حل چالش‌های امنیتی. -یادگیری از مثال‌های واقعی (حملات سایبری). -ایجاد محیط روانی امن برای گزارش‌دهی.
فرهنگ و یادگیری	آموزش	-آموزش‌های مستمر و دوره‌ای برای همه سطوح. -استفاده از روش‌های متنوع (ویدئو، اینفوگرافیک، کارگاه). - آموزش تجربه‌محور با تحلیل حوادث واقعی.
	گزارش‌دهی و شفافیت	-ایجاد کانال‌های اختصاصی برای گزارش‌دهی. -تشویق گزارش‌دهی سریع و بدون ترس. -استفاده از ابزارهای تحلیل لاگ (مثل SIEM).
	فرهنگ‌سازمانی	-امنیت به‌عنوان یک ارزش سازمانی. -مسئولیت‌پذیری جمعی (امنیت وظیفه همه است). -الگوسازی مدیران ارشد. -یادگیری از خطاها بدون تنبیه.
فرآیندهای شبکه‌سازی	ارتباطات غیررسمی	-تأثیر گفت‌وگوهای غیررسمی در فرهنگ‌سازی امنیتی. -اشتراک تجربیات واقعی بین همکاران. -نقش شبکه‌های ارتباطی در هماهنگی بین واحدها.
	ارتباطات عمودی	-جریان تصمیم‌گیری بین سطوح فنی و مدیریتی. -مشارکت ذی‌نفعان در کمیته‌های امنیتی.

مؤلفه‌های غیرانسانی در جدول (۲) در زیر نشان داده‌شده است:

جدول (۲). مؤلفه‌های غیرانسانی مؤثر در فرهنگ امنیت اطلاعات بر اساس نظریه انت

رده اصلی	زیررده	یافته‌های کلیدی
ساختارها و منابع	چالش‌های بودجه و منابع	-کمبود بودجه برای به‌روزرسانی ابزارها و سیستم‌های قدیمی. -کمبود نیروی انسانی متخصص. - تأخیر در به‌روزرسانی سیستم‌ها به دلیل محدودیت‌های مالی.
	تجهیزات قدیمی	-استفاده از سیستم‌های قدیمی که وصله‌های امنیتی برای آن‌ها منتشر نمی‌شود. -ناسازگاری سیستم‌های قدیمی با فناوری‌های جدید.
	کدهای تعاملی	ابزارهای انضباطی فناورانه
	کنشگران نهادی	-برنامه‌های تدریجی برای نوسازی سیستم‌ها. -آموزش مستمر کارکنان برای استفاده از ابزارهای جدید.
فرآیندهای سازمانی	آموزش مستمر	-برگزاری دوره‌های آموزشی ادواری برای کارکنان. -جلسات بازخورد برای بهبود فرآیندها.
	مکانیزم‌های بازتولید فرهنگ	-مشارکت کارکنان در جلسات آموزشی و مطالعه دستورالعمل‌های امنیتی. -ایجاد عادت‌های امنیتی در کارکنان.
زیرساخت‌های ارتباطی	اتصالات هم‌تخصصی	-تعامل مستمر بین بخش‌های مختلف فناوری اطلاعات. -شفافیت و ارتباط مؤثر برای اشتراک تجربیات و گزارش تهدیدات.
	جریان اطلاعات سلسله‌مراتبی	-گزارش سریع مشکلات به تیم پشتیبانی. -حمایت مدیریت ارشد از فرآیندهای امنیتی.
تأثیر فناوری بر فرهنگ	تبدیل امنیت به روال روزمره	-استفاده از فناوری‌هایی مانند لاگین دومرحله‌ای و رمزنگاری خودکار. -تبدیل امنیت از یک موضوع انتزاعی به بخشی از کارهای روزمره.
	اجرای خودکار سیاست‌ها	-استفاده از سامانه‌های رمزگذاری خودکار. -محدودیت‌های فناورانه برای جلوگیری از کپی فایل‌ها روی فلش‌درایوهای غیرایمن.
سیاست‌ها و مقررات	کنشگران هنجارساز	-سیاست‌های امنیتی روشن و تعریف‌شده. -انطباق با استانداردهای بین‌المللی مانند ISO 27001 .
	محرک‌های رفتاری	-تغییر دوره‌ای رمزهای عبور. -الزام به استفاده از VPN برای دسترسی خارج از سازمان.
فناوری‌های امنیتی	ابزارهای حفاظتی	-استفاده از آنتی‌ویروس، فایروال و سیستم‌های تشخیص نفوذ. -مدیریت وصله‌های امنیتی (patch management) -الگوریتم‌های یادگیری ماشین - نرم‌افزارهای DLP (Data Loss Prevention) - سیستم تشخیص نفوذ (IDS)
	کنترل‌کننده‌های دسترسی	-محدودیت دسترسی بر اساس نقش شغلی (RBAC). -استفاده از توکن‌های امنیتی و رمزهای یک‌بارمصرف. - سیستم‌های مدیریت دسترسی و هویت (IAM)

مؤلفه‌های تعامل انسان-فناوری به شرح جدول (۳) هست:

جدول (۳). مؤلفه‌های تعامل انسان-فناوری (مؤلفه‌های هیبرید)

رده اصلی	زیررده	یافته‌های کلیدی
سازگاری	سازگاری فناوری با نیازهای کاربران	"ابزارهای مدیریت رمز عبور کار را راحت‌تر کرده‌اند"
		"سیستم به کاربر یاد می‌دهد چه چیزی درست است"
	تنش‌های رابط	"پیچیدگی ابزارها خودش یک مانع است"
	تعادل کارایی-امنیت	"بین امنیت و کارایی باید تعادل برقرار کنیم"
	انعطاف‌پذیری فناوری	"استفاده از ابزارهای واسط برای پل زدن بین سیستم‌های قدیمی و جدید"
	تطبیق‌پذیری رفتار	"احراز هویت دومرحله‌ای پس از آموزش به رفتار عادی تبدیل شد"
	تأثیر فناوری بر رفتار	"لاگ‌گیری اول استرس‌زا بود، اما اکنون حس امنیت می‌دهد"
	یادگیری سازمانی	"ولی چون با دلایل منطقی و مستند مطرح شد، الان دیگه خودش شده بخشی از عرف کاری ما."
تعارض	مقاومت انسانی و کاربران	"بعضی افراد راهکارهای غیررسمی برای دور زدن محدودیت‌ها پیدا می‌کنند"
	مقاومت در برابر فناوری	"سیاست‌های امنیتی در ابتدا وقت‌گیر به نظر می‌رسند"
همکاری	هماهنگی بین‌واحدی	"جلسات مشترک با نماینده امنیت اطلاعات از ابتدای پروژه
	یادگیری جمعی	"جلسات داخلی برای توضیح فواید امنیت برای همه"

بحث و نتیجه‌گیری

این مطالعه با بهره‌گیری از نظریه کنشگر-شبکه به استخراج مؤلفه‌های انسانی و غیرانسانی شکل‌دهنده فرهنگ امنیت اطلاعات پرداخته است. یافته‌ها نشان می‌دهد که فرهنگ امنیتی محصول تعامل پویای شبکه‌ای از کنشگران انسانی و غیرانسانی است که در ادامه به‌تفصیل تحلیل می‌شوند.

۱. مؤلفه‌های انسانی مؤثر در فرهنگ امنیت اطلاعات

بر اساس تحلیل داده‌های کیفی، سه گروه کنشگر انسانی نقش محوری در شکل‌گیری فرهنگ امنیتی ایفا می‌کنند:

الف) مدیران ارشد (کنشگران راهبردی):

- نقش کلیدی در تصمیم‌گیری‌های استراتژیک و تخصیص منابع ("بودجه‌های امنیتی رو من باید تأیید کنم")
- عملکرد آن‌ها به‌عنوان الگوی رفتاری تأثیر مستقیم بر پذیرش سیاست‌ها دارد ("وقتی مدیران بالا رعایت امنیت رو جدی می‌گیرن...")
- مسئول فرهنگ‌سازی سازمانی از طریق حمایت آشکار از سیاست‌ها ("ساختن یه فرهنگ امنیتی تو سازمانه")

ب) کارکنان (کنشگران اجرایی):

- رفتارهای روزمره آن‌ها خط مقدم دفاع امنیتی است ("نباید هیچ فایل ناشناسی رو باز کنیم")
- سطح آگاهی و مسئولیت‌پذیری فردی تعیین‌کننده اثربخشی سیاست‌هاست ("احساس می‌کنم همه‌مون یه جورایی نقش داریم")
- گزارش‌دهی به‌موقع تهدیدات از ویژگی‌های کلیدی است ("سریع گزارش دادن")

ج) تیم‌های فنی (کنشگران واسط):

- ترجمه سیاست‌ها به راهکارهای عملیاتی ("حتی اصطلاحات امنیتی رو به زبان غیر فنی توضیح بدیم")
- پاسخ به حوادث و مدیریت بحران ("بررسی لاگ‌ها هنگام بروز اختلال")

- آموزش مستمر کاربران ("ما هر چند وقت یه بار یه سری پیام‌های آموزشی...داریم")

۲. مؤلفه‌های غیرانسانی مؤثر در فرهنگ امنیت اطلاعات

یافته‌ها پنج دسته از کنشگران غیرانسانی را شناسایی کرده‌اند که به‌طور فعال در شکل‌گیری فرهنگ امنیتی مشارکت دارند:

الف) سیاست‌ها و استانداردها:

- چارچوب‌های هنجاری مانند ITIL و ISO 27001
- دستورالعمل‌های اجرایی ("سیاست ممنوعیت USB")
- مکانیزم‌های انضباطی ("الزام تغییر دوره‌ای رمز عبور")

ب) فناوری‌های امنیتی:

- ابزارهای نظارتی مانند SIEM و DLP ("سامانه تشخیص ناهنجاری")
- سیستم‌های احراز هویت ("لاگین دومرحله‌ای")
- محدودیت‌های فناورانه ("سیستم اجازه نمی‌ده اطلاعات رو توی فلش بریزی")

ج) زیرساخت‌های فنی:

- شبکه‌ها و سخت‌افزارها ("تجهیزات ذخیره‌سازی")
- پلتفرم‌های ارتباطی ("VPN و دورکاری")

د) اسناد و پروتکل‌ها"

- مستندات خط‌مشی (بیانیه خط‌مشی امنیت اطلاعات بانک)
- دستورالعمل‌های عملیاتی ("چک‌لیست‌های امنیتی")

ه) فرآیندهای سازمانی:

- رویه‌های گزارش‌دهی ("گزارش بدون ترس از تنبیه")
- چرخه‌های بازخورد ("فرم‌های بازخورد")

۳. تعاملات انسان-فناوری به‌عنوان کنشگران هیبریدی در فرهنگ امنیت اطلاعات

یافته‌های این مطالعه نشان می‌دهد که برخی از مؤثرترین مؤلفه‌های شکل‌دهنده فرهنگ امنیت اطلاعات، در مرز بین کنشگران انسانی و غیرانسانی قرار می‌گیرند. این کنشگران هیبریدی که ترکیبی از انسان و فناوری هستند، در سه قالب کلی مشاهده شدند:

الف) فناوری‌های تغییردهنده رفتار

سیستم‌هایی مانند احراز هویت چندعاملی *(MFA)* یا سامانه‌های نظارتی *(SIEM)* نه‌تنها به‌عنوان ابزارهای فنی عمل می‌کنند، بلکه رفتار کاربران را مستقیماً تحت تأثیر قرار می‌دهند.

مثال: کاربران اشاره کردند که «اجباری شدن MFA در ابتدا چالش‌برانگیز بود، اما به‌تدریج به بخشی از عادات کاری تبدیل شد».

ب) سیاست‌های اجراشده توسط فناوری

خط‌مشی‌های امنیتی (مانند محدودیت استفاده از USB) زمانی مؤثر هستند که توسط فناوری‌ها (مثل رمزنگاری خودکار) پیاده‌سازی شوند.

مثال: «سیستم به‌طور خودکار از کپی داده‌ها روی حافظه‌های خارجی جلوگیری می‌کند».

ج) فرآیندهای یادگیری سازمانی

ابزارهای آموزشی (مانند شبیه‌سازی حملات فیشینگ) به‌عنوان کنشگران غیرانسانی، دانش امنیتی را به کاربران (کنشگران انسانی) منتقل می‌کنند.

این کنشگران هیبریدی نشان می‌دهند که مرز بین انسان و فناوری در فرهنگ امنیت اطلاعات سیال است و بهبود فرهنگ امنیتی نیازمند توجه هم‌زمان به هر دو بعد است.

تفاوت یافته‌ها با مدل‌های سنتی و پیشینه ادبیات موضوع

در جدول (۴) مقایسه‌ای میان رویکرد و رویه استخراج مؤلفه‌های مؤثر در فرهنگ امنیت اطلاعات بین مدل‌های سنتی و نظریه کنشگر-شبکه (انت) بررسی‌شده است.

جدول (۴). مقایسه رویکرد انت با مدل‌های سنتی در شناسایی مؤلفه‌های دخیل در فرهنگ امنیت اطلاعات

مؤلفه مقایسه	مدل‌های سنتی (هافستد[۷۷]، ۲۰۱۱، شاین، شلینگر-تویفل)	رویکرد انت در این مقاله
محوریت تحلیل	انسان‌محور (تمرکز بر ارزش‌ها/باورهای انسانی)	تقارن انسان و غیرانسان (فناوری، سیاست‌ها، زیرساخت‌ها به‌عنوان کنشگران فعال)
نقش فناوری	ابزار منفعل (بازتاب فرهنگ انسانی)	عامل تغییردهنده رفتار (مثال: SIEMها رفتار گزارش‌دهی را شکل می‌دهند)
فرآیند تغییر فرهنگ	خطی (آموزش ← تغییر نگرش ← تغییر رفتار)	شبکه‌ای و غیرخطی (تعامل پویای انسان-فناوری-سیاست)
تبیین مقاومت	ضعیف (معمولاً به‌عنوان مانع دیده می‌شود)	بخشی طبیعی از فرآیند ترجمه (مثال: مقاومت در برابر MFA نشانه تعامل کنشگران است)
روش بهبود فرهنگ	تأکید بر آموزش و رهبری	طراحی مجدد شبکه کنشگران (مثال: کاربرپسندسازی فناوری‌ها + بازطراحی فرآیندها)
مثال بارز	هافستد: فاصله قدرت بر پذیرش سیاست‌ها اثر می‌گذارد شلینگر-تویفل: سه‌گانه دانش-نگرش-رفتار	سیستم‌های احراز هویت چندعاملی (MFA) به‌عنوان کنشگران غیرانسانی، هنجارها را بازتعریف می‌کنند

این پژوهش با به‌کارگیری نظریه کنشگر-شبکه (انت)، درکی شبکه‌ای و پویا از فرهنگ امنیت اطلاعات ارائه کرد که در آن این فرهنگ، نه یک محصول نهایی، بلکه برآیند مستمر تعاملات و مذاکرات بین کنشگران انسانی و غیرانسانی است. برخلاف مدل‌های سنتی که فرهنگ امنیتی را خطی و سلسله‌مراتبی می‌بینند، پژوهش حاضر سه ویژگی کلیدی را برجسته می‌سازد:

۱- تقارن بنیادی و عاملیت توزیع‌شده: پژوهش نشان می‌دهد که عاملیت تنها در اختیار مدیران انسانی نیست. یک سیاست مکتوب (غیرانسانی) می‌تواند با الزام‌آور کردن رفتار، یک کنشگر قوی باشد. در مقابل، یک فناوری پیچیده (غیرانسانی) اگر

[77] Hofstede

با مقاومت کاربران (انسان) مواجه شود، می‌تواند عاملیت خود را از دست بدهد. فرهنگ امنیتی مؤثر، حاصل تعادل و هم‌ترازی عاملیت در سراسر این شبکه است.

۲- مرزهای سیال و کنشگران هیبریدی: پژوهش به‌وضوح مرز بین انسان و فناوری را در هم می‌شکند. کنشگرانی مانند «سیستم احراز هویت دومرحله‌ای»، ماهیتی دوگانه دارند: آن‌ها هم یک فناوری هستند و هم به‌طور فعال بر رفتار و عادات کاربر (انسان) تأثیر می‌گذارند و آن را بازتعریف می‌کنند. موفقیت این کنشگران هیبریدی، نقطه کلیدی در تحول فرهنگ امنیتی است.

۳- فرهنگ به‌مثابه فرآیند « ترجمه »: یافته‌ها نشان می‌دهد فرهنگ امنیتی موفق، نتیجه یک فرآیند «ترجمه» کارآمد است؛ یعنی تبدیل سیاست‌های سطح کلان (مانند ISO 27001) به رفتارهای روزمره توسط تیم‌های فنی و از طریق ابزارهای کاربرپسند. شکست در این فرآیند (مثلاً وقتی سیاست‌ها به‌درستی به فناوری یا آموزش ترجمه نمی‌شوند) منجر به مقاومت و تضعیف شبکه می‌شود. چالش«امنیت در مقابل کارایی» نیز درواقع یک تعارض در فرآیند ترجمه توسط کنشگران مختلف است.

از دیدگاه نظری، این پژوهش نشان می‌دهد که نظریه انت با رد دوگانگی انسان/فناوری، ابزار تحلیلی قدرتمندی برای کالبدشکافی پیچیدگی‌های فرهنگ امنیت اطلاعات فراهم می‌کند. از دیدگاه عملی، یافته‌ها، سه راهکار کلیدی را پیشنهاد می‌دهد:

مهندسی مجدد شبکه: به‌جای تمرکز صرف بر آموزش کارکنان، سازمان‌ها باید « شبکه کنشگران » خود را طراحی مجدد کنند. این کار شامل «کاربرپسندسازی فناوری‌ها» (تقویت کنشگران غیرانسانی)، شفاف‌سازی سیاست‌ها (تقویت کنشگران هنجارساز) و ایجاد کانال‌های ارتباطی مؤثر (تقویت پیوندهای بین کنشگران انسانی) است.

مدیریت مقاومت به‌عنوان نشانه: مقاومت در برابر تغییر (مانند مخالفت با MFA) نباید صرفاً به‌عنوان یک مانع دیده شود، بلکه یک نشانه ارزشمند از « تعارض منافع » یا « شکست در ترجمه درون شبکه » است. این مقاومت باید مورد تحلیل قرار گیرد تا نقاط ضعف شبکه شناسایی و برطرف شود. چارچوب پیشنهادی به سازمان‌ها کمک می‌کند تا با نگاهی همه‌جانبه، نقاط قوت و ضعف فرهنگ امنیتی خود را نه در افراد یا فناوری به‌تنهایی، بلکه در کیفیت تعاملات بین تمامی اجزای شبکه جستجو کنند.

درنهایت، این مطالعه گامی به‌سوی درکی سیال‌تر و مبتنی بر شبکه از فرهنگ امنیت اطلاعات برداشته است. این یافته‌ها می‌توانند مبنایی برای توسعه مدل‌های آینده و طراحی راهکارهای مؤثرتر در حوزه امنیت اطلاعات قرار گیرند. پیشنهاد می‌شود پژوهش‌های آتی با ترکیب روش‌های کیفی و کمی، به توسعه‌ی این چارچوب در بسترهای مختلف ادامه دهند.

پیروی از اصول اخلاق پژوهش

نویسندگان اصول اخلاقی را در انجام و انتشار این پژوهش علمی رعایت نموده‌اند و این موضوع مورد تأیید همه آن‌هاست.

مشارکت نویسندگان

نویسنده اول: تهیه و آماده‌سازی نمونه‌ها، انجام آزمایش و گردآوری داده‌ها، انجام محاسبات، تجزیه‌وتحلیل آماری داده‌ها، تحلیل و تفسیر اطلاعات و نتایج، تهیه پیش‌نویس مقاله.

نویسنده دوم: استاد راهنمای رساله، طراحی پژوهش، نظارت بر مراحل انجام پژوهش، بررسی و کنترل نتایج، اصلاح، بازبینی و نهایی‌سازی مقاله.

نویسنده سوم: استاد مشاور رساله، مشارکت در طراحی پژوهش، نظارت بر پژوهش، مطالعه و بازبینی مقاله

تعارض منافع

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

سپاسگزاری

از جناب آقای دکتر شریف‌زاده، استاد راهنمای رساله اینجانب و همچنین جناب آقای دکتر پورابراهیمی، استاد مشاور رساله، به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.

همچنین از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌گردد.

منابع

اسماعیلی, محبوبه, قلی زاده, محمدحسن, مرادی, محمود و ابراهیم پور ازبری, مصطفی. (۱۴۰۱). آینده‌پژوهی استفاده از فناوری بلاکچین جهت تسهیل مدیریت اطلاعات در سازمان تأمین اجتماعی با رویکرد کنشگر-شبکه. *پژوهشنامه پردازش و مدیریت اطلاعات*, ۳۸(۱), ۲۴۷-۲۷۰. doi: 10.35050/JIPM010.2022.021

جعفرنژآد ثانی, سهیلا , تقوا, محمدرضا , تقوی فرد, محمدتقی و سیدنقوی, میرعلی. (۱۴۰۲). ابعاد و مؤلفه‌های فرهنگ امنیت اطلاعات: یک مرور سیستماتیک. *پژوهشنامه پردازش و مدیریت اطلاعات*, ۳۸(۴), ۱۲۵۷-۱۲۸۱. doi:10.22034/jipm.2023.706394

رستمی, حمیدرضا , الهی, شعبان , معینی, علی و حسن‌زاده, علیرضا. (۱۴۰۱). روش‌شناسی کنش‌گر-شبکه در مطالعات علم و فناوری. *مطالعات مدیریت کسب‌وکار هوشمند*, ۱۰(۴۰), ۱۰۹-۱۳۳. doi: 10.22054/ims.2022.61719.1996

نازی، ایوب، حیدری، غلامرضا، و شریف‌زاده، رحمان. (۱۳۹۹). مدل متقارن تعامل اطلاعاتی: بازتعریفی از جایگاه فناوری در تعامل اطلاعاتی. *مطالعات کتابداری و سازمان‌دهی اطلاعات (مطالعات ملی کتابداری و سازمان‌دهی اطلاعات)*، ۳۱(۴ (پیاپی ۱۲۴))، ۱۱۴-۱۳۵. SID. https://sid.ir/paper/956956/fa

هاشمیان, سیدمحمدحسین و انواری, محمدرضا . (۱۳۹۷). دلالت‌های نظریه کنشگر شبکه در سیاست‌گذاری فرهنگی: تعامل تکنولوژی و انسان در سیاست‌گذاری. *دوفصلنامه علمی پژوهشی دین و سیاست فرهنگی*, ۵(۱), ۳۷-۶۴.

References

Alam, RG & Faruq, Amrul & Effendy, Machmud. (2025). Cybersecurity Management Strategies for Smart Cities in Indonesia: Cultural Factors and Implementation Challenges. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control. 10.22219/kinetik.v10i3.2226.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: a behaviour compliance conceptual framework. In Proceedings of the 8th Australasian Information Security Conference (AISC 2010) (Vol. 105, pp. 47-55). University of Southern Queensland.

Alharahsheh, H. H., & Pius, A. (2020). A review of key paradigms: Positivism VS interpretivism. Global academic journal of humanities and social sciences, 2(3), 39-43.

AlHogail, A., & Mirza, A. (2015). Organizational information security culture assessment. In Proceedings of the International Conference on Security and Management (SAM) (p. 286). The

Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
Alnatheer, M. A. (2014). A conceptual model to understand information security culture. International Journal of Social Science and Humanity, 4(2), 104.
Alnatheer, M., & Nelson, K. (2009). Proposed framework for understanding information security culture and practices in the Saudi context.
Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.
Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. European Journal of International Security, 1(2), 176-198.
Baron, L. F., & Gomez, R. (2016). The associations between technologies and societies: the utility of actor-network theory. Science, Technology and Society, 21(2), 129-148.
Bencherki, N. 2017. Actor–Network Theory. In Craig Scott & Laurie Lewis (eds.), The International Encyclopedia of Organizational Communication. New York, NY: Wiley. http://doi.org/10.1002/9781118955567.wbieoc002
Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: a tool to enhance trustworthiness or merely a nod to validation?. Qualitative health research, 26(13), 1802-1811.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
Braun, V., & Clarke, V. (2021). Thematic analysis: A practical guide.
Braun, V., Clarke, V., & Rance, N. (2014). How to use thematic analysis with interview data. The counselling & psychotherapy research handbook, 3, 183-197.
Callon, M., & Latour, B. (1981). Unscrewing the big Leviathan: how actors macro-structure reality and how sociologists help them to do so. Advances in social theory and methodology: Toward an integration of micro-and macro-sociologies, 1, 277-303.
Carter, N. (2014). The use of triangulation in qualitative research. Number 5/September 2014, 41(5), 545-547.
Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial management & data systems, 107(3), 438-458.
Chen, Y. A. N., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. Journal of Computer Information Systems, 55(3), 11-19.
Creswell, J. W., & Poth, C. N. (2016). Qualitative inquiry and research design: Choosing among five approaches. Sage publications.
Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & security, 29(2), 196-207.
Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713.
Darby, J.L., Fugate, B.S., & Murray, J.B. (2019). Interpretive Research. Approaches and Processes of Social Science Research.
De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. Electronics, 12(8), 1920.
Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering information security culture in small and medium size enterprises: an interpretive study in Australia.
Ernest Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial management & data systems, 107(3), 438-458.
Esmaili, M. , Qolizade, M. H. , Moradi, M. and Ebrahim pour Azbari, M. (2022). study of the future of using blockchain technology to facilitate information management in the organization.

Iranian Journal of Information Processing and Management, 38(1), 247-270. doi: 10.35050/JIPM010.2022.021. (in Persian)
Gichuru, M. J. (2017). The interpretive research paradigm: A critical review of is research methodologies. International Journal of Innovative Research and Advanced Studies (IJIRAS), 4(2), 1-5.
Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. Field methods, 18(1), 59-82.
hashemian, & anvari. (2018). Implications of Actor network Theory in Cultural Policymaking: Interaction of Technology and Humans in Policymaking. Bi-Quarterly Scientific Research Journal of Religion and Cultural Politics, 37-64. (in persian)
Hassan, N. H., & Ismail, Z. (2012). A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia-Social and Behavioral Sciences, 65, 1007-1012.
Hay, A. (2025). What may be: policy enactment in education, a new conceptual framework with actor-network theory. Journal of Education Policy, 40(2), 179-198.
Hedström, K., Dhillon, G., & Karlsson, F. (2010). Using actor network theory to understand information security management. In Security and Privacy–Silver Linings in the Cloud: 25th IFIP TC-11 International Information Security Conference, SEC 2010, Held as Part of WCC 2010, Brisbane, Australia, September 20-23, 2010. Proceedings 25 (pp. 43-54). Springer Berlin Heidelberg.
Hengstler, S., & Pryazhnykova, N. (2021). Reviewing the Interrelation Between Information Security and Culture: Toward an Agenda for Future Research. CIISR@Wirtschaftsinformatik.
Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. Online readings in psychology and culture, 2(1), 8.
Iskanderov, Y., & Pautov, M. (2020). Comprehensive Intelligent Information Security Management System (CIISMS) for Supply Networks: The Actor-Network Perspective. In Software Engineering Perspectives in Intelligent Systems: Proceedings of 4th Computational Methods in Systems and Software 2020, Vol. 1 4 (pp. 130-142). Springer International Publishing.
Jafarnezhad Sany, S. , Taghva, M. , Taghavifard, M. T. and Seyednaghavi, M. (2023). Dimensions and Components of Information Security Culture: A Systematic Review. Iranian Journal of Information Processing and Management, 38(4), 1257-1281. doi: 10.22034/jipm.2023.706394 (in Persian)
Jelani, A. (2021). Interpreting Human Societies and Social Dynamics through Multifaceted Exploration of Anthropological Frameworks. Social Science Chronicle, 1, 1-17.
Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. Information & Computer Security, 31(4), 463-477.
Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. Information & Computer Security, 23(3), 246-285.
Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. Information & Computer Security, 30(3), 382-401.
Kivunja, C., & Kuyini, A. B. (2017). Understanding and applying research paradigms in educational contexts. International Journal of higher education, 6(5), 26-41.
Labafi, S. (2020). Iranian data protection policy in social media; an actor-network theory approach. In Contemporary applications of actor network theory (pp. 121-139). Singapore: Springer Nature Singapore.
Latour, B. (1996). On actor-network theory: A few clarifications. Soziale welt, 369-381.
Law, J. (2008). Actor network theory and material semiotics. The new Blackwell companion to social theory, 141-158.
Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. (2010). Embedding information security culture emerging concerns and challenges.

Luxi, Tan. (2023). Actor-Network Theory. Sociology, doi: 10.1093/obo/9780199756384-0266
Martins, A., & Eloff, J. (2002, July). Assessing Information Security Culture. In ISSA (pp. 1-14).
Martins, N., & Da Veiga, A. (2015). An Information Security Culture Model Validated with Structural Equation Modelling. In HAISA (pp. 11-21).
Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. Computers & Security, 136, 103489.
Nazi , A., Heidari , g., & Sharifzadeh , R. (2021). Symmetrical Model of Information Interactions: Redefining the Weight of Technology in Information Interactions. Library Studies and Information Organization, 114-135. (in Persian)
Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. Holistica Journal of Business and Public Administration, 13(1), 49-72.
Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. Computers & Security, 108, 102340.
Okigui, H. H. (2023). An analysis of cyber-security policy compliance in organisations (Doctoral dissertation, Cape Peninsula University of Technology).
Orehek, Š., & Petrič, G. (2021). A systematic review of scales for measuring information security culture. Information & Computer Security, 29(1), 133-158.
Parsons, K., Young, E.G., Butavicius, M.A., McCormac, A., Pattinson, M.R., & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. Journal of Cognitive Engineering and Decision Making, 9, 117 - 129.
Rostami, H., Elahi, S., Moeini, A., & Hassanzadeh, A. (2022). Actor-Network Methodology in Science and Technology Studies. Business Intelligence Management Studies, 10(40), 109-133. (in Persian)
Safitra, M.F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability.
Sandelowski, M. (1995). Sample size in qualitative research. Research in nursing & health, 18(2), 179-183.
Santos, K. D. S., Ribeiro, M. C., Queiroga, D. E. U. D., Silva, I. A. P. D., & Ferreira, S. M. S. (2020). The use of multiple triangulations as a validation strategy in a qualitative study. Ciencia & saude coletiva, 25, 655-664.
Santos, R. E., Magalhães, C. V., & Da Silva, F. Q. (2017, November). Member checking in software engineering research: Lessons learned from an industrial case study. In 2017 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM) (pp. 187-192). IEEE.
Sas, M., Hardyns, W., Van Nunen, K., Reniers, G., & Ponnet, K. (2021). Measuring the security culture in organizations: a systematic overview of existing tools. Security Journal, 34(2), 340-357.
Schein, E. H. (1983). Organizational Culture: A Dynamic Model (No. TR13ONR).
Schein, E. H. (2010). Organizational culture and leadership (Vol. 2). John Wiley & Sons.
Schlienger, T., & Teufel, S. (2003). Information security culture-from analysis to change. South African Computer Journal, 2003(31), 46-52.
Schlienger, T., & Teufel, S. (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.
Shahri, A. B., Ismail, Z., & Rahim, N. Z. A. (2013). Security culture and security awareness as the basic factors for security effectiveness in health information systems. Sains Humanika, 64.(۲)
sharifzadeh, r., & moghadam heydari, g. (2015). From the social construction of knowledge to the collective construction of reality: Latour versus Bloor. Humanities Methodology, 93-120.
Shkarlet, S., Lytvynov, V., Dorosh, M., Trunova, E., & Voitsekhovska, M. (2019, June). The model of information security culture level estimation of organization. In International scientific-practical conference (pp. 249-258). Cham: Springer International Publishing.

Solomon, G., & Brown, I. (2020). The influence of organisational culture and information security culture on employee compliance behaviour. J. Enterp. Inf. Manag., 34, 1203-1228.

Soyref, M. and Seltsikas, P. (2014). Towards a holistic understanding of security process: formal controls and informal relationships.. https://doi.org/10.1109/hicss.2014.601

Sreeramagiri, P., Andrews, G., Greene, A. K., & Balasubramanian, G. (2022). Analyzing Security Risks in Cyber-Physical Manufacturing Systems with Actor–Network Theory. Smart and Sustainable Manufacturing Systems, 6(1), 110-121.

Tang, M., Li, M. G., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. Information Technology and Management, 17, 179-186.

Tatnall, A. (Ed.). (2012). Social influences on information and communication technology innovations. IGI Global.

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. Information & Management, 60(3), 1–20. https://doi.org/10.1016/j.im.2022.103751

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. Information Technology & People, 25(3), 327-352.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387.

Van de Kerke, T. W., & Hijzen, C. W. (2021). Secrecy, evidence, and fear: exploring the construction of intelligence power with Actor-Network Theory (ANT). Intelligence and National Security, 36(4), 527-540.

van der Wagen, W., & Pieters, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. European Journal of Criminology, 17(4), 480-497.

Walsham, G. (1997). Actor-network theory and is research: current status and future prospects., 466-480. https://doi.org/10.1007/978-0-387-35309-8_23

Zanke, A., Weber, T., Dornheim, P., & Engel, M. (2024). Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments. Computers & Security, 103938.

Zyoud, B., & Lutfi, S. L. (2024). The Role of Information Security Culture in Zero Trust Adoption: Insights from UAE Organizations. IEEE Access.