IREM International Review of Economics and Management
ISSN 2148-3493

Citation:Şeker, C. 2025. Cybercrimes In Organizations: Communication, Trust, And Leadership Approaches. *International Review of Economics and Management, 13(1), 31-50.* Doi: http://dx.doi.org/10.18825/iremjournal.1687722

CYBERCRIMES IN ORGANIZATIONS: COMMUNICATION, TRUST, AND LEADERSHIP APPROACHES

Cemile ŞEKER[1]

Başvuru Tarihi: 30 / 04 / 2025–Kabul Tarihi: 18 / 06 / 2025

Abstract

This study explores the role of leadership styles, organizational trust, and communication strategies in preventing cybercrimes within organizations. Based on a literature review, it finds that transformational and ethical leadership enhance trust and cybersecurity resilience, while authoritarian leadership harms communication and trust. Open and trustbased communication increases employee awareness and reduces ethical misconducts. The study emphasizes the need for integrated leadership, trust, and communication strategies to effectively combat cyber threats. According to findings, organizational trust, leadership characteristics, and trustful communication management are of utmost importance in preventing cybercrimes. Ethical and transformational leadership enhance trust, and information sharing among employees, making a strong immune system against cyberattacks. The trust culture increases employees' awareness of cybersecurity as well as reduces ethical misconducts. Open communication strengthens trust so that it will be easier to prevent such violations. Therefore, the simultaneous implementation of leadership, trust, and communication strategies enhances organizations' cybercrime resilience.

Keywords: Cybercrimes, Leadership Approaches, Transformational Leadership, Authoritarian Leadership, Trust Theory

Jel Classification: M14, D83, L86

Article Type: Review Article

[1] Dr. Lecturer, Near East University, Faculty of Tourism, Tourism Research Center, Nicosia, TRNC, cemile.seker@neu.edu.tr, https://orcid.org/0000-0002-69150-6845

KURUMLARDA SİBER SUÇLAR: İLETİŞİM, GÜVEN VE LİDERLİK YAKLAŞIMLARI

Öz

Bu çalışma, kurumlarda siber suçların önlenmesinde liderlik tarzlarının, örgütsel güvenin ve iletişim stratejilerinin rolünü incelemektedir. Literatür taramasına dayanan çalışmada, dönüşümcü ve etik liderliğin güveni ve siber güvenlik direncini artırdığı, otoriter liderliğin ise iletişim ve güveni zedelediği sonucuna ulaşılmıştır. Açık ve güven temelli iletişim, çalışan farkındalığını artırmakta ve etik dışı davranışları azaltmaktadır. Çalışma, siber tehditlerle etkin mücadele için liderlik, güven ve iletişim stratejilerinin entegre bir biçimde uygulanması gerektiğini vurgulamaktadır. Bulgulara göre, örgütsel güven, liderlik özellikleri ve güvene dayalı iletişim yönetimi, siber suçların önlenmesinde son derece önemlidir. Etik ve dönüşümcü liderlik, çalışanlar arasında güveni ve bilgi paylaşımını artırarak siber saldırılara karşı güçlü bir bağışıklık sistemi oluşturmaktadır. Güven kültürü, çalışanların siber güvenlik konusundaki farkındalığını artırmakta ve etik dışı davranışları azaltmaktadır. Açık iletişim güveni güçlendirerek bu tür ihlallerin önlenmesini kolaylaştırmaktadır. Bu nedenle, liderlik, güven ve iletişim stratejilerinin eş zamanlı uygulanması, kurumların siber suçlara karşı dayanıklılığını artırmaktadır.

Anahtar Kelimeler: Siber Suçlar, Liderlik Yaklaşımları, Dönüşümcü Liderlik, Otoriter Liderlik, Güven Teorisi

Jel Sınıflandırması: M14, D83, L86

Makale Türü: Derleme

I. INTRODUCTION

In the contemporary digital landscape, cybercrimes have evolved into significant security threats. The incidence of cyberattacks has increased dramatically in recent years, interfering with business operations, causing financial losses, and—most importantly—undermining stakeholder trust. A notable example of this phenomenon is the Colonial Pipeline ransomware attack of 2021, which resulted in the disruption of fuel supply chains in the United States and the exposure of systemic cybersecurity vulnerabilities. A similar situation was caused by the WannaCry attack in 2017, which affected over 200,000 computers in 150 countries, severely impacting public services and healthcare systems. In 2023, phishing-based breaches in European universities and hospitals raised further alarms about communication and data protection. These incidents demonstrate how deficiencies in leadership, communication, and organisational trust can amplify the repercussions of cyber threats. In the contemporary era, characterised by the perpetual progression of technology and digitalisation, it is imperative that organisational frameworks designed to combat cybercrimes are subject to constant evolution. It is imperative to rethink leadership strategies, internal communication practices, and trust-based governance in order to create resilient digital infrastructures.

Information technology (IT) is an essential tool for organizations in today's world. IT system risk management is a critical component in offering IT system security. Information security risk management is important for organizations to maintain operational effectiveness and security. In addition to offering organizations secure data to operate with, it guarantees data accuracy and retrievability. In order to mitigate cybersecurity attacks, regular risk assessment and countermeasure should be undertaken. There must be effective risk management plan for IT infrastructures to enable organizations to be able to prepare against cyberattacks. Organizations should be regularly analyzing and updating their risk management protocols in order to enhance their level of cybersecurity. This enables organizations to prepare not only for today's threats but for tomorrow's threats as well (Stoneburner et al., 2002). Organizations can benefit from leadership approaches to eliminate cybersecurity threats since leadership approaches can play an important role in building resistance against cybercrimes.

Transformational leadership fosters trust among employees, hence making the organization resilient against cyberattacks, whereas authoritarian styles of leadership can lead to mistrust and communication issues. Transformational leaders inspire and challenge their employees visionarily, which leads to organizational effectiveness. Visionary traits such as developing vision, supporting employee growth, innovativeness, change leadership, and establishing trust are inherent characteristics of transformational leadership (Sashkin, 2004; Şeker, 2024). Conversely, authoritarian leadership pursues a controlling and hierarchical style whereby the leader makes decisions autonomously and limits the participation of lowerlevel employees. Authoritarian leaders operate centrally, and they prefer not to listen to employees' ideas and only want the employees to take given work and execute it. Authoritarian leaders also demand a high level of obedience and discipline, and as such, this may suppress employees from speaking up. Communication is usually oneway, with little opportunity for employees to provide feedback or participate in decisionmaking. This kind of leadership style, which is characterized by strict control and low flexibility, can negatively influence employee satisfaction, motivation, and creativity (Harms et al., 2018).

Organizations must balance existing strategies with an open attitude towards innovative transformations in order to effectively deal with processes of fast change and innovation. This also means the requirement of a dynamic organizational structure (Tushman & O'Reilly, 1996; Şeker, 2024). Ethical leaders maintain high morals and inspire other people. They encourage employees to demonstrate ethical behavior, make them aware of their ethical responsibilities, and provide them with opportunities to carry out these responsibilities. Ethical leadership is also based on fair and transparent management; leaders clearly declare their decisions and inform employees about them. Ethical leaders do not just consider the interests of the organization but also examine the ethical implications of their decisions, taking into account ethical outcomes. Honesty and trust are core components of moral leadership; moral leaders set up trustworthiness and show candor in relations. Also, moral leaders consider the social impact of their organizations and embrace social responsibility, considering not only the wellbeing of individuals within the organization but society as a whole (Brown & Treviño, 2006).For this purpose, open, transparent, and trustbased leadership styles that facilitate communication can go a long way in sensitizing employees about cybercrimes as well as enhancing organizational security. Ethical and transformational leadership can be specifically seen as imperative strategies for cybercrime avoidance.

The present study examines the impact of cybercrimes in organisations in terms of communication, trust and leadership, and analyses feasible solutions for mitigating such threats. The proliferation of cyberattacks, both in terms of frequency and severity, has given rise to significant concerns regarding trust, operational disruption, and financial losses across diverse sectors. The study draws upon the principles of Trust Theory (Mayer et al., 1995) to emphasise how interpersonal and organisational trust can serve as a deterrent to ethical misconduct and as a catalyst for increased compliance with cybersecurity protocols. Moreover, the research is informed by the principles of Transformational Leadership Theory (Bass & Riggio, 2006), which posits that inspirational and supportive leaders can enhance employee awareness and responsibility within digital environments. The conceptual model proposed in this study explores how ethical and transformational leadership styles contribute to organisational trust, and how both trust and internal communication quality affect an organisation's capacity to prevent cybercrimes. The relationships in question are examined through the lens of a theoretically grounded model, with a view to offering insight into leadership-based prevention strategies.

The present research was conducted exclusively on the basis of a systematic literature review. A comprehensive and interdisciplinary coverage of scholarly publications was ensured by utilising worldwide academic databases, including Web of Science (WoS), Scopus, ScienceDirect, Google Scholar, EBSCOhost, ProQuest, and Taylor & Francis Online. The selection of these databases was based on several key criteria, including their extensive indexing of peer-reviewed journals, their global scope, and their relevance to the fields of management, organisational studies, leadership, and cybersecurity. WoS and Scopus were favoured due to their citation indexing capabilities and bibliometric strength, while databases such as ScienceDirect and Taylor & Francis were included due to their specialised content in leadership and organisational behaviour. The literature review was guided by key terms such as "cybercrimes", "organizational trust", "transformational leadership", "authoritarian leadership", "internal communication", and "cybersecurity strategy". The inclusion criteria for publications were as follows: firstly, that they be peer-reviewed; secondly, that they be published in English; and thirdly, that they fall within the specified time frame of 2010 to 2024. Thematic and conceptual relevance to the intersection of leadership, trust, communication, and cybersecurity constituted the primary inclusion criterion.

The findings of the literature review indicate that transformational and moral leadership styles significantly enhance organisational trust and contribute to building resilience against cybercrimes. For instance, Haney and Lutters' (2025) research posits that security awareness programmes that prioritise behavioural modification – typically supported by transformational leadership – demonstrate superior efficacy in comparison to those that are exclusively focused on compliance. In a similar vein, Uchendu, Nurse, and Bada (2021) underscored the pivotal role of top-down leadership support and transparent communication in nurturing a robust cybersecurity culture. Conversely, authoritarian leadership has been linked to elevated levels of communication breakdowns and trust deficits, which can compromise cybersecurity preparedness (Vrhovec & Markelj, 2024). Furthermore, Bada, Sasse, and Nurse (2019) advanced the argument that awareness campaigns lacking leadership involvement and trust-based communication often fail to yield sustainable behavioural change among employees.

Accordingly, the study emphasizes the necessity to implement transformational and ethical leadership approaches, form communication policies that create trust, and prioritize inhouse awareness schemes to control cybercrimes. The study emphasizes the necessity to conduct more research on cybercrimes in the context of leadership and trust and recommends organizations develop good leadership and communication strategies in order to become more robust.

II. MATERIALS AND METHODS

This study was conducted using the review (literature review) approach. Review studies critically examine previous research on a particular topic area, summarizing, comparing, and combining the literature relevant to the field (Snyder, 2019). Literature reviews are carried out in order to compile information already available on a study topic, demonstrate the situation within a field, stipulate areas of ignorance, and guide possible future studies (Webster & Watson, 2002). A literature review provides the potential to evaluate research in a systematic context and examine different aspects of a topic (Okoli & Schabram, 2010). There are several important reasons for choosing a literature review as the methodology of this study:

1. Synthesizing and Evaluating Existing Knowledge: The best way to examine all existing studies on a particular topic and to access accumulated knowledge is by conducting literature review. All three of the terms to be discussed latercybercrime, leadership style, and organizational trustcarry significant literature. Conducting literature review synthesizes existing studies in the provided fields to achieve a superior level of understanding of the topic at hand (Hart, 1998).

2. Presenting Alternative Perspectives and New Methodologies: Literature review compares the outcome of different studies, presenting multiple perspectives and opinions on a topic. For instance, when examining the effect of transformational and authoritarian types of leadership on cybercrime, comparing what many authors have to say could be helpful in broadening understanding (Booth et al., 2021).

3. Thorough Analysis of the Research Subject: A literature review is useful in understanding the past evolution, current applications, and future research in a given topic. In rapidly evolving areas like cybercrime, a summary of existing studies ensures access to new information. Additionally, understanding the relationship between leadership and trust is very useful in analyzing organizational behavior (Cooper, 1989).

4. Effective Use of Time and Resources: Literature review is most appropriate for research under time and resource limitations. The project of a comprehensive literature review makes effective use of knowledge that is already available before conducting new data gathering. This enables the research to be accomplished more quickly and at less expense (Fink, 2019).

5. Research Gap Identification: One identifies research gaps through a literature review, in which previous research is lacking or incomplete, providing an opportunity for new research. Such a review may help identify the research gaps on cybercrime and organizational trust and provide a foundation for future research (Tranfield et al., 2003).

6. Between Constructing Theoretical Framework: A study needs a review of literature to develop its theoretical framework. Trust theory, leadership models, and communication planning can be better established on the bases of literature so that scientific contributions towards a study are supplemented (Cronin, 2011).

In this study, the literature was searched according to international academic indexes such as Web of Science (WoS), Scopus, Science Direct, Google Scholar, EBSCOhost, ProQuest, and Taylor & Francis Online. During the searching process, the key words such as cybercrime, organizational trust, leadership styles, transformational leadership, authoritarian leadership, organizational communication, cybersecurity, trust theory, communication strategies, trust in organizations, and leadership and trust relationship were identified. Recent research papers were examined to contrast the roles of leadership styles in fighting cybercrime, the effects of trust on institutions, and how communication strategies are involved in cybersecurity.

III. CYBERCRIME AND EFFECTS ON ORGANIZATIONS

Cybercrime are criminal acts that arise out of information technology misapplication. The criminal acts come in varied forms such as cyberattacks, data theft, and identity theft. At organizations, cybercrime leads to erosion of trust, disruption of business processes, and financial loss. The impact of cybercrime does not just come in the form of direct financial loss but also impacts negatively on staff morale and motivation, leading to a decrease in organizational productivity in general.

The effects of cybercrime extend beyond organizational losses; they also negatively affect the external reputation of an organization. Organizations that have been targeted by cyberattacks or data breaches stand to lose their customers' and stakeholders' trust, which is a form of longterm reputation loss (Kshetri, 2017). Aside from monetary losses, cybercrime negatively affects the psychological and social wellbeing of individuals. Such offenses harm the reputation of the organization and destroy trust, causing loss of customers and financial losses in the long run. Moreover, preventing cybercrime effectively must establish a strong cybersecurity framework and minimize possible security loopholes. In the process, creating awareness among people and employees regarding cybercrime is significant. On this note, raising awareness of cybersecurity is an important strategy in reversing the effects of cybercrime (Saini et al., 2012).

Cybercrime poses a very serious problem to organizations, and many of these challenges emerge while dealing with it. Das & Nayak (2013) identify not just the monetary, legal, and social effects of cybercrime but also those that need to be developed so as to counter such crimes. From their studies, cybercrime not only incurs economic costs but also negatively impacts organizational reputation, leading to loss of trust over the long term. That is not quite true, however, since such crimes are preventable via cybersecurity and good strategy. Aside from that, cybercrime prevention requires not just technical solutions, but also organizational and cultural change (Das & Nayak, 2013).

Monies expended to combat cybercrimes within organizations impose financial burdens and destabilise managerial functioning further. In order to counter such crimes and their effects, organizations must embrace cybersecurity practices and instill trust culture. Leadership patterns are crucial in this context. Transformational leadership has proven more effective than other forms of leadership in establishing trust and raising employee awareness (Bass & Avolio, 1994). Developing an effective working space and resistance against cybercrime might mean adopting open communication methods.

Leadership styles play an important role in determining the organizational trust climate, which in turn determines cybercrime prevention. Transformational leadership supports trust by enhancing employees' organizational performance commitment (Sashkin, 2004), and thus it is an effective leadership style for preventing cybercrime. Authoritarian leadership with a more authoritarian control style may lead to trust deficiencies and communication problems (Hollander & Offermann, 1990), potentially leading to greater cybercrime. Ethical leadership can have a negative impact on cybercrimes because it creates an ethical culture in organizations.

IV. TRUST THEORY, ORGANIZATIONAL TRUST, AND COMMUNICATION STRATEGIES

Trust Theory provides a theory of explaining trust relationships between people. Organizational trust is critical in the battle against cybercrime within organizations. Organizational trust is the foundation for successful collaboration and good working relationships within a firm. The combined model of trust by Mayer et al.,(1995) suggests three important components of trust: competence, integrity, and benevolence. This model is interested in understanding how people and groups establish trust with each other and also how trust affects organizational behaviors. Trust directly affects most organizational aspects such as leadership, job satisfaction, and performance, which ultimately influence organizational success. Through the process, establishing a good trust environment aids in making organizations more efficient and sustainable (Mayer et al., 1995).

Trust fosters cooperation and information sharing among organizational members, and this can enhance the prevention and detection of cybercrimes. Organizational trust is a key pillar that constructs cooperation and business efficiency among employees. The presence of trust enables employees to cooperate more easily and effectively with one another and managers, thereby strengthening organizational loyalty. But when this trust is broken, it can lead to firm conflicts, demotivation, and performance decline. Therefore, developing strategic means of building and maintaining trust is necessary to guarantee organizational longterm success (Calton, 1998). Organizational trust weakening can hinder information sharing among employees and reveal security threats.

Trust promotes teamwork and information sharing within an organization, thus helping to prevent and detect cybercrimes. Organizational low trust hinders the sharing of information and speeds up security threats. Establishing a secure environment raises employees' alertness to cybercrimes and directs them toward appropriate behaviors. Organizational trust is a crucial factor that has a direct effect on employees' risktaking attitudes and work performance. It is shaped by individuals' perception of the reliability of their managers and colleagues, and this perception is a key driver in organizational commitment, job satisfaction, and performance. Employees are likely to take the initiative and make bold decisions in the face of uncertainties and dangers in environments where there exists high trust. Conversely, in lowtrust organizations, workers will act more cautiously and will overlook innovative and initiative approaches. Therefore, adopting a leadership style encouraging trust is considered a main component in improving workers' job performance (Colquitt et al., 2007).

It is achievable to uphold trust in organizations if leaders adhere to a fair and transparent mindset towards the workers. This supports the firm's security culture and renders it a stronger system against cybercrimes. Leadership trust has a direct impact on important factors such as employee performance, organizational commitment, and job satisfaction. In workplaces where there exist high trust environments, employee’s exhibit greater loyalty to leaders, whereas low levels of trust can lead to work stress, communications breakdown, and reduced productivity. As leaders exhibit fairness, consistency, and support in their processes of establishing trust, employees' trust in leadership becomes reinforced, resulting in enhanced organizational effectiveness. In addition, the effect of leadership trust may vary depending on organizational culture, communication flows, and individual trust propensity (Dirks & Ferrin, 2002).

Besides, within hightrust culture, workers take greater responsibility and are more active in doing things for security. Within organizational context, employees' behavior that is observable toward managers and colleagues determines the establishment of trust. Trust stimulates workers' tendency to collaborate, assume risks, and engage in open communication, while distrust negatively affects job performance and organizational commitment. Gillespie's (2003) Behavioral Trust Inventory (BTI) provides a concrete framework for measuring trust in organizational relationships and determining how trust is manifested in interpersonal relationships. In this regard, developing strategies to establish trust in organizations can positively impact employee performance and job satisfaction (Gillespie, 2003).

The level of trust in organizations dictates the quality of managerial decisionmaking processes. In hightrust organizations, information sharing is clearer, cooperation is greater, and decisionmaking is of a better quality. In lowtrust environments, workers tend to withhold information, suspicion becomes normal, and decisionmaking processes are undermined, resulting in low organizational effectiveness. Therefore, managers must develop a culture in which trust is at the center, since it has the power to significantly impact organizational performance (Zand, 1972).With this, not only can building a trusting environment in organizations be able to stop cybercrimes, but also workplace productivity is enhanced.

Communication initiatives enhance the effectiveness of cybersecurity procedures and maintain the trust of the organization. Transparent, open communication increases workers' awareness concerning cybercrimes, and as a result of that, avert them. Efficient internal communication plays a central role in regard to increasing workers' motivation and work performance. Cowan (2014) discusses how successful internal communication management can boost the engagement and job performance of employees as well as emphasize the positive impact of effective internal communication methods on employee satisfaction and overall productivity. Similarly, Men (2014) examines the interrelationship between transformational leadership, channels of communication, and employee satisfaction, observing the significant impact of effective internal communication on job satisfaction. These researches highlight the internal communication role of building trust, commitment, and performance (Cowan, 2014; Men, 2014).

Where there is high trust, positive outcomes such as cooperation, knowledge sharing, and employees' high motivation emerge, whereas distrust cultures yield the lack of cooperation, communication breakdowns, and organizational conflicts. These dynamics highlight the importance of actions by leaders that seek to build trust and reduce distrust. Effective management of trust and distrust is therefore one of the determinants of organizational success and sustainability (Kramer, 1999). Effective communication strategies in this respect make the organization more open, enhancing the perception of trust among employees and reducing communication errors. Proper communication encourages employees to comply with security policies and provides them with sufficient information about the security practices of the organization. Open and regular communication also helps in implementing early warning systems to stem the impact of cybercrimes as the employees are more attuned to security breaches. Correspondingly, open communication within an organization not only makes individuals more sensitive but also assists in rendering the overall organizational structure more robust.

V. LEADERSHIP APPROACHES IN STRATEGIES FOR COMBATING CYBERCRIMES

For effective combat of cybercrimes, leadership, communication tactics, and trust need to be married together. Effective leadership tactics, such as transformational leadership, increase the climate for trust but also foster working cooperation and knowledge exchange among the staff (Bass, 1998). It can greatly help in curtailing cybercrimes. Besides that, ensuring safe channels of communication enables workers to receive faster and more accurate information on security threats, therefore curbing the impacts of cybercrimes. Organizations can mitigate the effects of cybercrimes and provide a safer working environment by adopting open communication policies, ethical and transformational leadership, and avoiding authoritarian leadership styles.

Transformational leadership is a leadership style that aims to inspire and empower employees by changing their values, beliefs, and behaviors. In this leadership style, not only does the leader lead the employees to perform their responsibilities, but also enhances their ability. Transformational leaders apply a visionary approach, develop an inspiring vision of organizational purpose in the future, and encourage employees to fulfill this purpose by informing them (Sashkin, 2004). Transformational leaders have charisma, intellectual stimulation, and individual consideration. Charismatic leaders utilize their position of leadership well to motivate organization members to direct themselves towards higher goals (Bass & Riggio, 2006). In addition, intellectual stimulation provides a setting in which employees can challenge their present mode of thinking and develop more innovative solutions.

Transformational leaders are interested in people in the organization, try to understand them, and assist them in development. This ensures workers to be more dedicated to work and facilitates the success of the organization. Transformational leadership further allows organizations to embrace change processes, hence promoting innovation (Northouse, 2018; Şeker, 2024). Transformational leadership application in organizations contributes to the improvement of the trust climate, increasing collaboration, and improving overall productivity (Judge& Piccolo, 2004; Şeker, 2024). Trustbased communication policies and transformational leadership have the capability to offer significant support towards averting cybercrimes in organizations. Moreover, enhancing awareness activities within organizations can lead to increased cybersecurity awareness among employees and a more robust resilient system against cybercrimes.

Ethical leadership is a form of leadership in which the leaders are concerned with creating an environment in their organizations based on justice, honesty, respect, and ethical principles. Ethical leadership involves leaders making the right decisions not only to achieve the objectives of the organization but also by considering the welfare of employees and the welfare of society (Brown et al., 2005). Ethical leaders maintain high standards of ethics in decisionmaking, establish such standards within their organizations, and expect the same from their employees (Northouse, 2018).

Ethical leadership is equally responsible for developing trust in an organization. Ethical leaders establish trust in the organization by their acceptance of a fair, open, and responsible method of operation and acting as a model of conduct for employees (Brown & Treviño, 2006). Ethical leaders help employees to adopt organizational values, execute tasks, and improve organizational loyalty. Ethical leadership makes sure that companies do not only work for profits but also with their social responsibilities in mind, thus making firms more sustainable and longterm achievements. Ethical leadership also positively influences employees' inworkplace conduct. Ethical leadership makes employees adhere more to moral principles at work, and it also averts moral deterioration, injustices, and abuses within the workplace (Mayer et al., 2012). Ethical leaders' capacity to guide the values and culture within the organization sustains employees' morale and leads to greater embracement of ethical values within the organization. Based on the literature review of ethical leadership, the following are the conclusions.

Ethical leadership can go a long way in preventing information technology (IT) crimes within organizations. Ethical leaders are leaders who adhere to high ethical standards and guide their employees by example by demonstrating to them the correct behavior. Such leaders adopt important values such as justice, honesty, and transparency in their organizations and teach employees to embrace these values. This type of leadership provides a firm foundation to guarantee that IT crimes are not committed. Ethical leadership helps to create a strong foundation of ethical values within the organizational culture, and such values are important factors in discouraging IT crimes. Ethical leaders render their employees aware of issues such as privacy, security, and protection of personal information. Ethical leaders foster a culture of responsibility and accountability within the organization, thus preventing the spread of IT crimes. These leaders also have zerotolerance policies for unethical behavior within the organization, which makes IT crimes more detectable and preventable. Besides, ethical leadership fosters trust among employees, and trust is a critical factor in preventing IT crimes. Ethical leaders create transparent communication and trustbased relationships and motivate employees to share information. Such an environment provides useful opportunities to identify and prevent potential IT crimes. Ethical leadership also fosters employees' cybersecurity awareness. Ethical leaders clearly communicate cybersecurity procedures and guidelines, motivating employees to follow such procedures. In this regard, ethical leadership creates a favorable climate to eradicate IT crimes among organizations and enables employees to behave ethically. This type of leadership results in organizations becoming immune to IT crimes.

Authoritarian leadership, on the other hand, is a leadership where the leader makes decisions without involving the employees in the decisionmaking process. In this leadership, the leader's control is better, and employees must play by some rules without being given the right to make independent decisions (Lewin et al., 1939). Employees are usually supposed to follow the directions of the leader, and such a leadership style is often seen in crisis situations with a formal organizational structure. Authoritarian leadership may be helpful in a crisis situation or when there is a need for quick decisions because the centralized leadership enables quick and accurate decisionmaking (Tannenbaum & Schmidt, 1973). However, over the long run, this kind of leadership has a negative influence on employees. The restriction of involvement and inhibition of creative thought can reduce workers' morale and motivation, which creates a decrease in productivity. In addition, authoritarian leaders fail to consider the views of their employees, creating organizational commitment loss and employee frustration. This leadership style also brings about communication failure, lack of cooperation, and trust issues. Authoritarian leadership, by not engaging employees in decisionmaking and imposing close supervision upon them, can adversely affect employees' work attachment and motivation. Authoritarian leadership, therefore, could lead to initial success but, in the long run, erodes employees' creative thinking and commitment (Goleman, 2017).

Authoritarian leadership is understood in terms of singlehanded decisionmaking by the leader, minimal employee involvement, and control of the leader over the organization. Authoritarian leadership promotes an inflexible hierarchical organizational culture as well as a rule of authoritybased order in the organizational framework. From all these remarks, it can be said that authoritarian leadership goes against preventing IT crimes in organizations. This kind of leadership stifles the freedom of employees to share information and hence erodes organizational trust. Secondly, the high level of control and low rates of collaboration involved by authoritarian leaders expose the organization to a high risk of cybersecurity breaches. The last factor contributing to authoritarian leadership's weak resistance to IT crime is the lack of trust nurtured by the leader. The workers will be less cooperative in an environment where they do not trust their leaders, and this encourages IT crimes like information leakage and data theft. Moreover, authoritarian leadership may restrict open communication channels within the organization, eliminating the sense of support, which lowers the willingness of the workers to report security breaches or other IT crimes. Research has found that workers' perceptions of support in the workplace highly influence their job attitudes. Perceived support has been found to be highly connected with many factors like job satisfaction, commitment of workers, motivation, and performance at work, as per many studies. All these findings indicate that organizations can influence workers' workplace attitudes and behaviors in a positive manner through a supportive workplace environment. Thus, managers' supportive behaviors are a critical factor for improving personal performance and organizational success (Ng & Sorensen, 2008). Supportive behaviors are possessed by the effective leader for the employees. Thus, IT crimes are prevented by organizations.

In Kirkpatrick and Locke (1996), three of the most critical aspects of charismatic leadership—vision, selfconfidence, and inspiration—were assessed for direct and indirect effects on attitudes and performance. According to the study, the leadership factors show the way in which a leader guides organizational excellence and improves employees' job attitudes and performance. The study reveals that charismatic leadership improves employees' motivation, which in turn increases their job commitment and productivity. With this in mind, effective leadership does not only influence individual performance but also the success of an organization. As a result, within organizations, effective leadership can create a culture where IT crimes are prevented through the establishment of trust and communication and the positive influence on attitudes and behavior.

VI. DISCUSSION AND SUGGESTIONS

This study answers to the impact of cybercrimes on organizations and examines effective leadership styles, trust theory, and communication management approaches in addressing these crimes. The findings of the study determine that cybercrimes in organizations not only inflict financial loss but also broader effects like loss of trust, interruption of business processes, and motivation of employees. Against this background, leadership styles and organizational trust are matters of critical significance regarding the prevention of cybercrimes.

Transformational leadership, with enhanced organizational trust, promotes transparency and sharing of information among employees (Bass, 1999). From the study, it is learned that transformational leaders build a robust organizational platform against cybercrimes and enhance employees' security awareness. However, authoritarian leadership has been presumed to bring distrust, hence communication problems and difficulty in preventing cybercrimes. This is because this form of leadership negatively affects the trust climate and communication (Goleman, 2017). The findings from the study show that ethical leadership has the potential to reduce cybercrimes in the organization because ethical leaders create a trust climate through fairness and honesty to their employees (Brown & Treviño, 2006). This trust increases employees' commitment towards their organizations and hence minimizes ethical violations. Ethical leaders promote good behaviors by example, openness, and accountability. With this, it is difficult to promote bad behaviors such as cybercrimes, and a stronger ethical culture is established within the organization. Ethical leadership also lays a foundation that makes employees report potential crimes, thus it is essential to detect and prevent cybercrimes. It is an important measure of the impact that leadership style has on an organization's climate of trust.

Organizational trust plays an important role in the prevention of cybercrimes. Trust theory identifies the fact that organizations with a trust environment are a strong determinant in identifying and preventing cybercrimes. Communication processes using trust methods are accountable for instilling a proactive behavior towards cybercrimes by raising the awareness level of employees about cybersecurity. In addition, it is also noted that open and transparent communication improves the extent of trust among employees, thus allowing them to avoid cybercrimes. As one of the best practices to combat cybercrimes, the integration of leadership and measures of trust together with the reinforcement of policy on communication is critical. Application of these practices enhances employees' cybersecurity awareness levels and makes the organization safe. In addition, increasing internal awareness exercises and performing regular training are great measures in the prevention of cybercrimes.

In conclusion, leadership strategies, trust strategies, and communication strategies together are needed to avert cybercrimes. This study emphasizes that organizations ought to build solid leadership and communication strategies so that they can prepare them to become more resilient. This research recommends the need to carry out further studies in the areas of leadership and trust for a better fight against cybercrimes. Subsequent research can contribute to the literature by examining the influence of different leadership styles, theories of trust, and communication measures on cybercrimes more comprehensively. In this context, the following recommendations can be made for organizations:

1. Adopting Transformational Leadership Styles: Organizations should adopt transformational leadership styles as a way of combating cybercrimes. Transformational leaders build trust within employees, foster open communication, and enhance organizational trust, thus making it simpler to identify and prevent cybercrimes. The leaders should also raise awareness about cybersecurity and grant employees the authority to promote secure behaviors.

2. Establishing TrustBased Communication Strategies: Trustbased communication strategies establish a culture of open and transparent communication within organizations. Trust development among employees raises cybersecurity awareness and assists in the

prevention of cybercrimes. Organizations must strengthen such communication strategies at the horizontal and vertical levels and encourage information sharing.

3. Synthesizing Trust and Leadership Strategies: A synthesis of trust and leadership strategies is required so that cybercrimes can be effectively combated. Trustfostering mechanisms heavily engage leaders. Leaders are required to learn how to instill trust, ensure transparency, and foster cybersecurity and incorporate such strategies into business culture.

4. Organizing Training and Awareness Programs: Regular cybersecurity training and awareness programs need to be organized to improve the employees' knowledge regarding cybercrimes, and they need to be addressed to employees at all levels. These programs assist in creating a stronger organizational structure against possible cyberattacks.

5. Updating Cybersecurity Protocols: Organizations should adopt modern and efficient cybersecurity protocols to deter cybercrimes. These protocols should possess strong data security controls, identity authentication, and network protection. Additionally, protocols should go through regular examination through continuous monitoring and testing procedures.

6. Promoting Open Information Sharing: Promoting open information sharing among organizations is one of the main causes in building trust among employees. To prevent cybercrimes, there need to be proper informationsharing platforms designed by the organizations in an open manner after having adopted confidentiality and security practices.

7. Internal Auditing and Risk Assessment Activities Investment: Firms have to improve internal auditing activities and create regular risk assessment processes in order to lower cybersecurity threats and prevent cybercrime. The audits help in the early detection of likely weak areas and security vulnerabilities.

8. Encouraging Employees' Ethical Conduct: Ethical leadership is essential to instill ethical conduct among employees. Organizations must have ethical codes and values, and the leaders must lead employees by example in carrying out their ethical roles. This can prevent cybercrimes from taking place.

9. Investment in Digital Innovation and Technological Investments: The dynamic nature of technology requires organizations to constantly upgrade their digital security systems. Organizations must invest in new technologies and continually improve their digital innovation process to create a stronger defense against cyberattacks.

10. Embracing Ethical Leadership: Ethical leadership is a framework that guides organizational behaviors and provides ethical values to employees. Ethical leaders establish a work culture founded on trust and accountability, and they play a very crucial role in stopping cybercrimes. Ethical leadership trains employees with appropriate behaviors and ensures they adhere to their ethical responsibilities, particularly with cybersecurity.

11. The study emphasizes the major role of leadership strategies and mechanisms of trust in the combating of cybercrimes. It emphasizes the importance of further research on the topic, especially prevention of cybercrimes within the paradigm of leadership and trust, for developing effective organizational strategies. The future research could help us know how different leadership strategies, mechanisms of trust, and their interaction with organizational culture can make the entire working of organizations strong.

These recommendations can help organizations become more resilient to cybercrimes and protect themselves from their negative effects.

REFERENCES

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.

Bass, B. M. (1999). Two decades of research and development in transformational leadership. European journal of work and organizational psychology, 8(1), 932.

Bass, B. M., & Avolio, B. J. (Eds.). (1994). Improving organizational effectiveness through transformational leadership. Sage.

Bass, B. M., & Riggio, R. E. (2006). Transformational leadership (2nd ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Bass. B. M. (1998). Transformational Leadership: Industrial, Military, and Educational Impact. Mahwah, NJ: Lawrence Erlbaum Associates.

Booth, A., James, M. S., Clowes, M., & Sutton, A. (2021). Systematic approaches to a successful literature review. Sage.

Brown, M. E., & Treviño, L. K. (2006). Ethical leadership: A review and future directions. The leadership quarterly, 17(6), 595616.

Brown, M. E., Treviño, L. K., & Harrison, D. A. (2005). Ethical leadership: A social learning perspective for construct development and testing. Organizational behavior and human decision processes, 97(2), 117134.

Calton, J. M. (1998). Trust in organizations: frontiers of theory and research. Business and society, 37(3), 342.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: a metaanalytic test of their unique relationships with risk taking and job performance. Journal of applied psychology, 92(4), 909.

Cooper, H. M. (1989). Integrating research: A guide for literature reviews (2nd ed.). Sage Publications.

Cowan, D. (2014). Strategic internal communication: How to build employee engagement and performance. Kogan Page.

Cronin, C. (2011). Doing your literature review: Traditional and systematic techniques. Evaluation & Research in Education, 24(3), 219–221

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142153.

Dirks, K. T., & Ferrin, D. L. (2002). Trust in leadership: metaanalytic findings and implications for research and practice. Journal of applied psychology, 87(4), 611628.

ENISA. (2023). Threat Landscape 2023 – Phishing incidents in EU universities and hospitals. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Fink, A. (2019). Conducting research literature reviews: From the internet to paper. Sage publications.

Gillespie, N. (2003). Measuring trust in working relationships: The behavioral trust inventory. Melbourne Business School.

Goldstein, M. (2021, May 10). Cyberattack forces shutdown of major U.S. fuel pipeline. The New York Times. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

Goleman, D. (2017). Leadership that gets results. In Leadership perspectives (pp. 8596). Routledge.

Haney, J., & Lutters, W. (2025). From compliance to impact: Tracing the transformation of an organisational security awareness programme. Cyber Security: A Peer-Reviewed Journal, 8(2), 110-130. https://doi.org/10.69554/NJYA9034

Harms, P. D., Wood, D., Landay, K., Lester, P. B., & Lester, G. V. (2018). Autocratic leaders and authoritarian followers revisited: A review and agenda for the future. The Leadership Quarterly, 29(1), 105122.

Hart, C. (1998). Doing a literature review: Releasing the social science research imagination. Sage.

Hollander, E. P., & Offermann, L. R. (1990). Power and leadership in organizations: Relationships in transition. American Psychologist, 45(2), 179–189.

Judge, T. A., & Piccolo, R. F. (2004). Transformational and transactional leadership: A metaanalytic test of their relative validity. Journal of Applied Psychology, 89(5), 755768.

Kirkpatrick, S. A., & Locke, E. A. (1996). Direct and indirect effects of three core charismatic leadership components on performance and attitudes. Journal of applied psychology, 81(1), 36.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. Annual review of psychology, 50(1), 569598.

Kshetri, N. (2017). 1 Cybercrime and Cybersecurity in the Global South. Springer.

Lewin, K., Lippitt, R., & White, R. K. (1939). Patterns of aggressive behavior in experimentally created "social climates". The Journal of social psychology, 10(2), 269299.

Mayer, D. M., Aquino, K., Greenbaum, R. L., & Kuenzi, M. (2012). Who displays ethical leadership, and why does it matter? An examination of antecedents and consequences of ethical leadership. Academy of management journal, 55(1), 151171.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 20(3), 709734.

Men, L. R. (2014). Strategic internal communication: Transformational leadership, communication channels, and employee satisfaction. Management communication quarterly, 28(2), 264284.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5), 1938-1940.

Ng, T. W. H., & Sorensen, K. L. (2008). Toward a further understanding of the relationships between perceptions of support and work attitudes: A metaanalysis. Group & Organization Management, 33(3), 243–268. https://doi.org/10.1177/1059601107313307

Northouse, P. G. (2018). Leadership: Theory and Practice (8th ed.). Sage Publications.

Okoli, C., & Schabram, K. (2015). A guide to conducting a systematic literature review of information systems research.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cybercrimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202209.

Sashkin, M. (2004). Transformational leadership approaches: A review and synthesis. In J.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333339.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. Nist special publication, 800(30), 80030.

Şeker, C. (2024). Örgütlerde değişime direnç performans ilişkisinde öğrenen örgüt algısı ve dönüşümcü liderliğin rolü (Doktora Tezi). Bandırma Onyedi Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Bandırma

Tannenbaum, R., & Schmidt, W. H. (1973). How to choose a leadership pattern. Harvard business review.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British journal of management, 14(3), 207222.

Tushman, M. L., & O'Reilly, C. A. III. (1996). Ambidextrous organizations: Managing evolutionary and revolutionary change. California Management Review, 38(4), 8–30.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

Vrhovec, S., & Markelj, B. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. Plos one, 19(10), e0312266. https://doi.org/10.1371/journal.pone.0312266

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly, xiiixxiii.

Zand, D. E. (1972). Trust and managerial problem solving. Administrative science quarterly, 229-239.