Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(8), 138-162
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Comprehensive Review of Cybersecurity for Modern Work: Attacks, Zero Trust and NIS2 Compliance

Cristina-Ioana Călin, Andreea-Mihaela Comșiț

Electrical Engineering and Computer Science Faculty, Transylvania University of Brasov, Brasov, Romania
Email: Email: andreea.calin@unitbv.ro

How to cite this paper: Călin, C.-I. and Comșiț, A.-M. (2025) A Comprehensive Review of Cybersecurity for Modern Work: Attacks, Zero Trust and NIS2 Compliance. *Journal of Computer and Communications*, **13**, 138-162.
https://doi.org/10.4236/jcc.2025.138007

Received: July 14, 2025
Accepted: August 12, 2025
Published: August 15, 2025

Abstract

The COVID-19 pandemic drastically altered traditional work environments, accelerating remote work adoption and exposing new cybersecurity vulnerabilities. This article analyzes the evolving threat landscape in both Work From Office (WFO) and Work from Home (WFH) contexts, focusing on the surge in phishing, ransomware, insider threats and attacks exploiting unsecured home networks and remote access protocols. To address these risks, organizations must move toward adaptive security frameworks such as Zero Trust Architecture, which assumes no implicit trust within or outside the network and enforces strict access controls. Additionally, the article explores the relevance of the updated NIS2 Directive, which expands regulatory scope and introduces stricter cybersecurity obligations across critical sectors in the European Union (EU). Together, Zero Trust and NIS2 serve as foundational pillars for securing hybrid work models and enhancing organizational resilience in the face of modern cyber threats.

Keywords

Cybersecurity, Zero Trust Architecture, NIS2, Identity and Access Management, Cloud Security, Risk Mitigation, “Never Trust, Always Verify”

1. Introduction

The COVID-19 pandemic marked a turning point in the way organizations operate, accelerating a global shift from traditional on-site work environments to remote and hybrid models. Prior to 2020, the majority of employees carried out their activities within the physical perimeter of company offices, where security policies

and infrastructures were centralized and strictly controlled [1]. However, the pandemic forced a sudden and large-scale adoption of work-from-home (WFH) practices, exposing numerous vulnerabilities in both technological infrastructure and user behavior [2].

As hybrid work becomes the new standard, cybersecurity threats have evolved in complexity and frequency. The traditional notion of a secure network perimeter is no longer sufficient in an environment where devices, users and data are distributed across diverse and often uncontrolled locations [3]. In this new paradigm, the user's identity has emerged as the primary security boundary, demanding new approaches to authentication, access control and threat mitigation [4].

According to Ahmad [5], cybercriminals are exploiting popular terms (example: COVID-19) in file names to deceive users into opening malicious files. For instance, a file named Eeskiri-COVID-19.chm ("eeskiri" meaning "rule" in Estonian) appears to be a helpful resource but is a keylogger. Once opened, it collects login credentials and sends the data to maildrive [.] icu. Using trending events in cyberattacks is a common tactic among threat actors, who often capitalize on timely news, holidays or celebrities in social engineering schemes. In the hurry to find helpful information, people may unwittingly expose sensitive data. In times of uncertainty, it's especially important to take a step back and think about who you can trust online.

Kotak *et al.* [6] provided key taxonomies and shared findings from a detailed risk analysis, highlighting threats, their impacts and mitigation strategies. The analysis uncovered various risks to corporate networks, especially from new attack vectors in remote work setups. Companies must assess remote work policies, limit access privileges, implement proper security tools and set clear risk-mitigation guidelines. Taxonomies should be regularly updated as threats evolve and risk scores will vary by organization based on preparedness, industry risk and employee roles.

WFH presents security issues such as: network security (WFH increases data risk without a secure network) [7], phishing and social engineering (the attackers trick users into sharing private data, causing data breaches) [8], password management (passwords should be complex and unique to each account to prevent unauthorized access) [9], endpoint security (update antivirus and firewall software on endpoints to protect against malware attacks.) [10], data protection (encrypt sensitive data, back it up regularly and use cloud storage and backup) [11] and video conferencing security (ensure secure, password-protected video meetings due to increased usage) [12].

Hui *et al.* [13] found that implementing international regulations, such as the Code of Conduct (COC), reduced the number of distributed denial of service (DDoS) attacks in enforcing countries by at least 11.8%. Many countries do not participate in international treaties for various reasons, including differing laws and the potential for discordance among international and domestic regulations. Campbell *et al.* [14] studied how security breach announcements affect market

value. They found that a breach of confidential information reduced a company's market value by 5%, whereas a breach of non-confidential information had a different impact. Gordon *et al.* [15] found that economic incentives encourage healthcare and financial organizations to implement information security controls like e Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley (GLB) Act.

Regulatory frameworks such as NIS2 Directive (EU 2022/2555) and architectural models like the Zero Trust Architecture (ZTA) are becoming essential for organizations aiming to maintain resilience, compliance and business continuity in a distributed work context [16]. Before implementing ZTA, organizations must assess risks to understand security, identify vulnerabilities and assess risks to critical systems. This helps ensure ZTA is applied effectively and focused on the areas of most concern [17].

Adopting ZTA is a cultural shift that requires continuous education and awareness. All employees must understand the principles of Zero Trust (ZT) and their role in protecting the organization from cyber threats and related attacks. Organizations should invest in regular, up-to-date cybersecurity training programs for employees [18]. These programs should cover ZTA principles such as the importance of identity verification, multi-factor authentication (MFA) and the concept of least privilege access. Training should also include recognizing and responding to cyber threats [19].

On July 6, 2016, the European Union (EU) adopted the Network and Information Systems (NIS) Directive to establish a unified cybersecurity policy. Recognizing the global and societal impact of cyberattacks, the directive aimed to provide a foundation for achieving a common cybersecurity level across the EU, considering the cross-border nature of cybersecurity [20]. However, its adoption exposed gaps in achieving consistent cybersecurity across member states. The updated NIS2 Directive broadens its scope, adds stricter requirements and emphasizes risk management, aligning with global cybersecurity standards and best practices [21].

This paper aims to provide:

1) A comparative analysis of the threats and vulnerabilities associated with Work from Office (WFO) and Work from Home (WFH), focusing on three distinct phases: before, during and after the COVID-19 pandemic.

2) It examines the evolution of cybersecurity strategies related to infrastructure security, identity protection and the implementation of modern security standards such as Zero Trust and NIS2.

This research is structured as follow: Section 2 represents the Methodology, Section 3 describes How Work Has Evolved: Before, During & After the COVID-19, Section 4 presents the Threats and Vulnerabilities for WFO and WFH, Section 5 presents Company Perimeter Security & User Identity Security, Section 6 describes ZTA, Section 7 describes NIS2 Directive, Section 8 represents the Discussions and Section 9 represents the Conclusions.

2. Methodology

To ensure the inclusion of the most reliable evidence and the identification of all relevant studies, we adopted a systematic approach throughout our research. This process involved implementing a comprehensive search strategy, carefully conducted in alignment with the literature search guidelines specified in reference [22] and the Preferred Reporting Items for Systematic Reviews (PRISMA) recommendations outlined in reference [23].

A ScienceDirect database search was used to identify relevant scientific literature. The search was limited to English-language publications and there were no restrictions on their geographical distribution between 2015 and 2024 to ensure data relevance and accuracy. The search query was performed using specific keywords in the title, abstract and keywords fields of the documents.

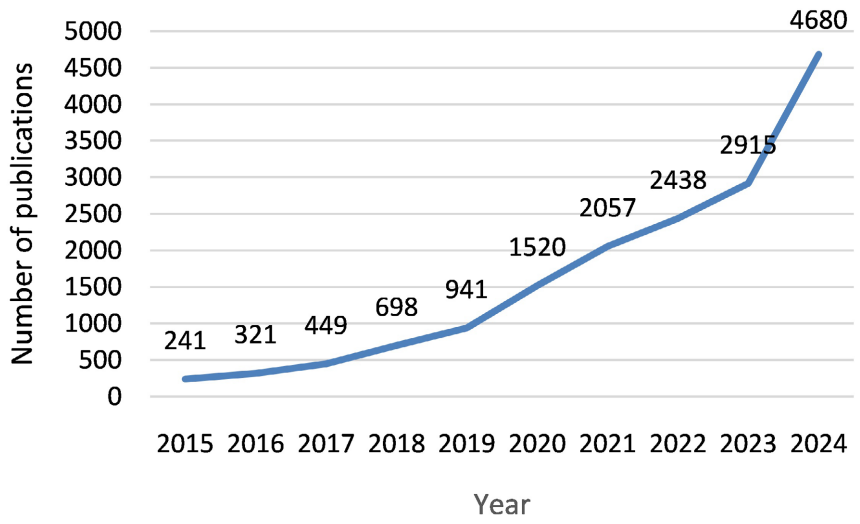

Figure 1. The number of published articles based on keyword "cybersecurity".

Figure 1 illustrates the trend in the number of published articles over the past ten years related to the keyword "cybersecurity" within the ScienceDirect database. The number of academic publications referencing the keyword "cybersecurity" has shown a steady and substantial increase over the past decade. In 2015, there were only 241 publications, but this number has risen significantly each year, reaching 4680 publications in 2024, representing an approximate 19-fold increase over the ten-year period. Between 2015 and 2019, the growth was gradual, with the number of publications rising from 241 to 941, indicating growing academic interest in the topic. A more pronounced acceleration is observed starting in 2020, likely influenced by the global digital transformation triggered by the COVID-19 pandemic and the rise of remote work, which brought cybersecurity to the forefront of both research and practice. The number of publications increased sharply from 1520 in 2020 to 2057 in 2021 and continued to rise in the following years, reaching 2915 in 2023. The most significant spike occurs in 2024, with 4680 publications, suggesting an ongoing intensification of research activity in this field,

possibly driven by the increasing complexity of cyber threats, the integration of AI in cybersecurity and regulatory pressures across industries.

Figure 2 illustrates the evolution of publications for the keywords “work from home” and “work from office” in the last 10 years. The comparative analysis of publication trends reveals a significant shift in academic interest toward the concept of "work from home", particularly beginning in 2020. From 2015 to 2019, the number of publications using the keyword “work from home” remained low and relatively stable, ranging from 4 to 9 publications annually, reflecting limited scholarly focus on remote work during that time. In contrast, the “work from office” keyword maintained a similarly low profile, fluctuating modestly between 4 and 12 publications per year. However, a sharp increase in publications related to “work from home” is observed starting in 2020, coinciding with the onset of the COVID-19 pandemic. Publications jumped from 9 in 2019 to 36 in 2020 and continued to surge in subsequent years, peaking at 175 in 2023, before slightly declining to 154 in 2024. This dramatic growth reflects the global transition to remote work and the corresponding surge in interest surrounding its implications for productivity, cybersecurity, mental health and workplace culture. Conversely, academic output related to “work from office” remained relatively stagnant during the same period, with slight fluctuations but no significant increase. Notably, post-2020, publications on “work from office” did not experience a resurgence despite the gradual return to physical workplaces, suggesting a sustained shift in research focus toward remote or hybrid work models.

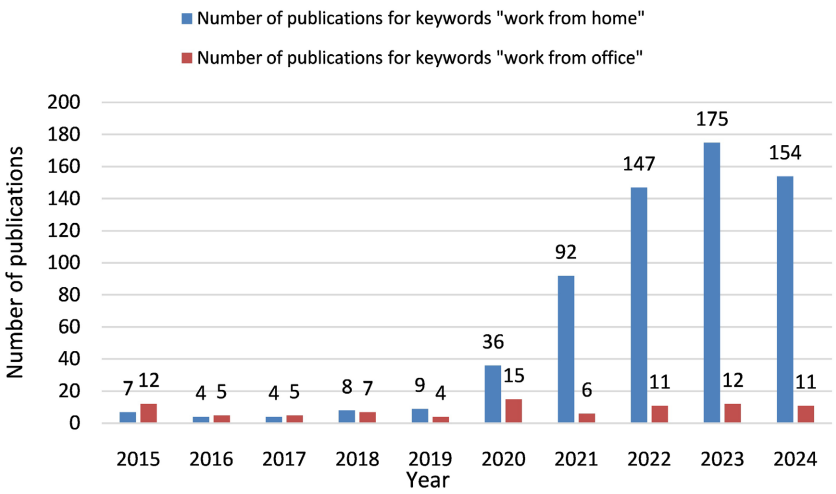

Figure 2. Number of publications for keywords “work from home” and “work from office”.

Figure 3 presents the evolution of the publications for keywords “Zero Trust Architecture”. The academic interest in ZTA has demonstrated a steady and persistent presence over the past decade, with fluctuations that reflect both evolving cybersecurity paradigms and contextual drivers such as organizational digital transformation and increased cyber threat exposure. From 2015 to 2019, the number of publications remained relatively stable, fluctuating between 165 and 210

articles per year. This indicates early recognition of ZTA concepts, although the research community had not yet broadly expanded its investigation during this phase. A notable shift begins in the post-2020 period. While 2020 saw a slight dip to 176 publications, subsequent years display a clear upward trajectory: 233 in 2021, 192 in 2022, 265 in 2023 and reaching a peak of 316 in 2024. This growing interest corresponds with heightened cybersecurity concerns triggered by increased remote work, the decentralization of IT environments and the expansion of cloud-based infrastructures, conditions that underscore the limitations of traditional perimeter-based security models and emphasize the relevance of ZTA. The sharp increase in 2023 and 2024 suggests that ZTA has transitioned from a niche or emerging topic to a mainstream framework within cybersecurity research. It reflects not only the maturing of the concept but also its growing adoption across sectors seeking robust security architectures resilient to insider threats, supply chain risks and sophisticated external attacks.

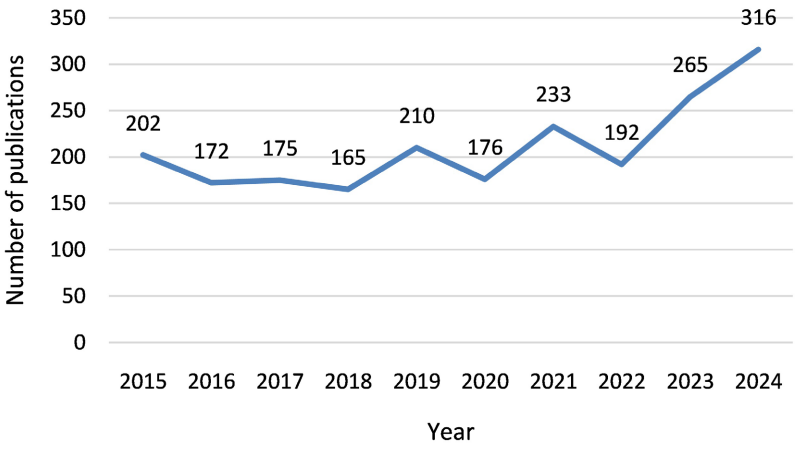

Figure 3. Number of publications for keywords "Zero Trust Architecture".

In addition to the bibliometric analysis, a thematic synthesis was employed to enhance the analytical rigor and support the systematic nature of this review. Following the identification of relevant literature, a qualitative assessment was conducted to extract and categorize recurring themes and focal areas within the body of work. Core topics such as ZTA and the NIS2 Directive were selected based on their frequency of appearance, relevance to contemporary cybersecurity discourse, and their citation in high-impact publications. A manual coding process facilitated the identification of thematic patterns related to regulatory evolution, architectural transformations in cybersecurity, and organizational responses to the rise of remote and hybrid work environments. This integrative approach enabled the derivation of meaningful insights that extend beyond publication trends, thereby reinforcing the methodological robustness of the review.

3. How Work Has Evolved: Before, during & after COVID-19

Prior to 2020, the dominant model of professional activity was grounded in the

physical presence of employees within organizational offices. This traditional work-from-office (WFO) approach allowed for centralized IT infrastructure, direct oversight of employees and strict control over access to resources. Security models were primarily based on perimeter defense, relying heavily on firewalls, internal network segmentation and physical access control [24]. Remote work was rare and often reserved for exceptional roles or senior staff and VPN access was highly restricted and tightly monitored.

Organizations before COVID-19 placed a significant emphasis on physical network security and endpoint protection within corporate environments. However, this perimeter-centric security model often failed to account for insider threats and lacked agility in adapting to mobile or cloud-based ecosystems [25].

The onset of the COVID-19 pandemic in early 2020 forced a massive and sudden transition to remote work on a global scale. Organizations had to rapidly reconfigure IT infrastructures to accommodate work-from-home (WFH) arrangements, often without proper planning or the implementation of robust security protocols [2]. In many cases, remote access was granted through hastily deployed VPNs and personal devices were allowed for work use without adequate endpoint security or monitoring.

This abrupt shift exposed organizations to a wide range of cybersecurity vulnerabilities. According to reference [26], cybercrime reports increased by over 300% during the early months of the pandemic, largely due to phishing attacks, ransomware and exploitation of unpatched systems. Employees working from home became primary targets due to weaker network protections and lower security awareness. The decentralization of the workforce also strained traditional IT support models, making it difficult for organizations to enforce compliance, manage devices or monitor user activity effectively [27].

In the post-pandemic period, many organizations have adopted hybrid work models, allowing employees to alternate between working from home and from the office. While this approach offers increased flexibility and productivity, it also introduces long-term cybersecurity challenges that must be addressed with strategic planning and modern frameworks [1].

The hybrid era has accelerated the adoption of cloud-first strategies, identity-centric security and Zero Trust Architecture (ZTA) as organizations acknowledge the dissolution of traditional network perimeters [28]. Additionally, regulatory compliance requirements such as those outlined in the NIS2 Directive, mandate higher levels of resilience, incident reporting and risk management across both public and private sectors [16].

As work becomes more decentralized, the need for continuous authentication, dynamic access policies and secure user behavior monitoring has become paramount. The security paradigm has shifted toward protecting data, users and devices, regardless of location, through real-time threat detection, micro-segmentation and least privilege access [3].

4. Threats and Vulnerabilities

As organizations adapt to flexible and hybrid work environments, the threat landscape has significantly evolved. Both WFO and WFH models present unique cybersecurity risks. This section compares the key threats and vulnerabilities inherent in each approach and highlights the underlying differences in security exposure and control.

4.1. Work from Office (WFO)

The traditional office environment allows centralized control of physical and digital assets. IT departments typically manage network infrastructure, deploy endpoint protection uniformly and restrict access to sensitive systems through internal firewalls and physical barriers [25]. Despite these advantages, WFO environments are not immune to cyber threats.

Key Threats and Vulnerabilities in WFO:

1) Insider Threats: Malicious or negligent insiders can exploit unrestricted internal access [29].

2) Phishing and Social Engineering: Email-based attacks targeting office employees remain prevalent and are often successful due to human error.

3) Lateral Movement: Once an attacker gains access to the internal network, poor segmentation allows easy movement between systems [30].

4) Removable Media Risks: USB devices and external storage used within the office can introduce malware into controlled environments [28].

5) Legacy Systems: Many on-premises environments rely on outdated systems that may lack security patches or modern authentication mechanisms [16].

While organizations benefit from physical security measures (example: key cards, surveillance), their dependency on perimeter-based security models makes them vulnerable when employees connect remotely or when boundaries are breached.

4.2. Work from Home (WFH)

The WFH model decentralizes control, shifting security responsibility partly to the end user. Employees connect through home networks and often use personal devices, increasing exposure to unmanaged risks [2].

Key Threats and Vulnerabilities in WFH:

1) Unsecured Networks: Home Wi-Fi networks often lack enterprise-grade encryption and firewall configurations.

2) Inadequate Endpoint Security: Personal devices may lack antivirus software, disk encryption or regular updates.

3) Credential Theft: Remote workers are more susceptible to phishing, credential stuffing and man-in-the-middle attacks [26].

4) Weak Authentication Mechanisms: Password reuse and lack of multi-factor authentication (MFA) significantly increase breach risk [4].

5) Shadow IT: Employees may use unauthorized applications (example: mes-

saging, file sharing tools) to bypass slow VPNs or access limitations [31].

6) Data Leakage: Working in uncontrolled environments increases the risk of accidental data exposure, such as through family members or unsecured file transfers.

According to a report by European Network and Information Security Agency's (ENISA) [16], organizations observed a sharp increase in attack vectors directly related to remote work conditions, particularly phishing campaigns exploiting pandemic-related themes and remote desktop protocol (RDP) attacks.

Hybrid work models demand a unified security strategy that addresses both environments while reducing reliance on traditional perimeter-based defenses [3]. This has led to a rise in identity-focused security models and Zero Trust adoption, explored in later sections. Table 1 presents a comparative summary of WFO and WFH.

Table 1. Comparative Summary—WFO vs WFH.

Aspect	WFO	WFH
Network Control	High—centralized and managed	Low—reliant on personal/home networks
Endpoint Security	Standardized company devices	Mixed—includes unmanaged personal devices
Physical Security	High—badge access, surveillance	Low—home environments vary
Identity Risk	Lower—on-prem MFA, physical identity checks	Higher—dependent on remote authentication
Threat Exposure	Lateral movement within internal network	Phishing, RDP exploits, unsecured Wi-Fi
User Monitoring	Continuous with corporate tools	Limited and privacy-restricted monitoring
Policy Enforcement	Centralized and enforced	Decentralized and inconsistent

4.3. Cyber-Attacks for WFO and WFH

The COVID-19 pandemic caused a dramatic shift in work environments, accelerating remote work adoption and reshaping cybersecurity risks [32]. Both traditional office-based (WFO) and remote (WFH) setups experienced an increase in cyber-attacks as threat actors exploited uncertainty, reduced IT oversight and global fear. Table 2 highlights the cyber-attacks which could appear in WFH and WFO setups.

Table 2. Comparative table highlighting the cyber-attacks that could occur in WFH vs WFO setups.

Cyber Attack Type	WFH	WFO	Comments
Phishing Emails	High risk due to less oversight and personal email usage	Moderate risk, filtered through corporate email systems	Common in both, but less monitored at home

Continued

Malware & Ransomware	High risk from unpatched personal devices and networks	Moderate risk; better controls like endpoint protection in place	Often spread via email or unverified downloads
Man-in-the-Middle (MitM)	High risk on unsecured home/ public Wi-Fi	Low risk with secure internal networks	VPNs are critical for WFH environments
Data Leakage	High risk via personal devices, cloud storage or USBs	Moderate risk due to centralized data control	Lack of Data Loss Prevention (DLP) tools at home increases risk
Insider Threats	Lower visibility, hard to monitor user behavior remotely	Easier to detect unusual behavior on-site	Insider threats remain significant in both
Credential Theft	High risk via phishing or reused passwords on home systems	Moderate risk, with SSO and MFA often enforced	MFA should be enforced in both settings
Shadow IT	High due to use of unauthorized tools/services by employees	Lower, with stricter IT policies and monitoring	Employees often install unsanctioned apps/tools at home
DDoS	Lower individual risk; higher risk to remote access infrastructure	Higher risk to centralized infrastructure	Company systems (VPN, email, etc.) are more targeted than individuals
Social Engineering	High risk due to isolation and lack of quick team consultation	Moderate risk, with ability to verify in person	Exploits psychological tactics; remote workers are more vulnerable
Unpatched Software	High risk from outdated personal OS/software	Lower risk with centralized patch management	Home systems may skip updates
Supply Chain Attacks	Medium risk; personal purchases or services may be compromised	Medium risk; relies on corporate vendor security	Not location-dependent, but WFH can introduce non-standard vendors/tools
Physical Security Breaches	Low in most WFH unless using shared/public spaces	High risk of unauthorized access without badge/ policies	Physical access risk flips based on environment

The shift to remote work has significantly expanded the cyberattack surface, exposing organizations to heightened risks such as phishing, ransomware and unsecured home networks. Research indicates that the rapid and often unplanned transition to WFH environments introduced inconsistent security practices and increased employee susceptibility to social engineering and endpoint exploitation. To effectively mitigate these evolving threats, a multi-layered cybersecurity approach is essential: one that incorporates VPNs, MFA, endpoint protection and comprehensive user awareness training (Table 3).

Table 3. Threats for WFO and WFH.

Reference	WFH/WFO	Description
[33]	WFO	Explores how in-office employees are vulnerable to manipulation via social media and workplace communication.
[34]	WFO	Assesses risks of personal device use within office environments.
[35]	WFO	Details cyber vulnerabilities in office-like academic environments.
[29]	WFO	Focuses on WFO risks from malicious or negligent insiders.
[36]	WFH	Identifies WFH/WFA cybersecurity challenges and organizational awareness; highlights the need for training and guidelines.
[37]	WFH	Evaluates new cyber risks in WFH setups (hurried tech deployments, privacy trade-offs).
[38]	WFH	Surveys COVID-19-related phishing, propaganda and malware targeting WFH workers.
[39]	WFH	Reviews risks from hybrid setups and recommends enterprise-level frameworks.
[40]	WFH	Highlights 500% surge in attacks during pandemic; emphasizes VPN, MFA, endpoint management.
[41]	WFH	Explores phishing, ransomware and human vulnerabilities within academic remote settings.
[42]	WFH	Qualitative interviews on employee views of remote work and its evolving cyber risks.

5. Company Perimeter Security & User Identity Security

The shift from centralized office work to hybrid and remote models has fundamentally changed the cybersecurity landscape. Traditional approaches focused on securing the organization's physical and network perimeter are no longer sufficient in a world where users, devices and applications operate from virtually anywhere. Consequently, organizations are transitioning from perimeter-based security to user identity–centric security, placing individual identity at the core of their security strategy.

5.1. Company Perimeter Security: Traditional Foundations and Emerging Challenges

Perimeter security is rooted in the assumption that threats originate from outside the organization's internal network, while users and systems inside are inherently trusted. Security teams typically employ tools like firewalls, Virtual Private Net-

works (VPNs) and Intrusion Detection Systems (IDS) to enforce this model [24].

The main characteristics of perimeter-based security include:

1) Centralized access control based on IP address and location [43].

2) Physical safeguards (example: badge access, secured data centers) [44].

3) Static rules for firewall and traffic filtering [45].

4) Device-centric policies, often limited to corporate-owned endpoints [46].

While effective in physically contained environments, this model exhibits serious limitations in the context of cloud adoption, mobile work and third-party integrations. Once an attacker breaches the perimeter via phishing, malware or a compromised VPN, they often encounter minimal resistance moving laterally across internal systems [28].

The COVID-19 pandemic accelerated the obsolescence of perimeter-based models. With millions of users connecting from untrusted locations and devices, organizations quickly realized that traditional perimeter defenses could not be scaled to secure a highly distributed workforce [16].

5.2. User Identity Security: A Modern Paradigm

User identity security centers on who the user is, rather than where they are connecting from. It leverages authentication, authorization and continuous monitoring to ensure that only verified and permitted users gain access to sensitive resources.

Core components of identity-centric security include:

1) MFA for robust identity verification. MFA adds a second or third layer of verification such as: biometrics or app-based tokens, making it significantly harder for attackers to use stolen credentials [47].

2) Single Sign-On (SSO) to unify credentials across systems [48].

3) Identity and Access Management (IAM) for lifecycle control of user privileges [49]. IAM platforms enforce role-based access control (RBAC), least privilege principles and timely deprovisioning of unused accounts, especially crucial in managing employee onboarding or offboarding cycles [50].

4) Behavioral analytics to detect anomalies in user activity [51].

5) Context-aware access based on device health, location and risk score [52].

6) User Behavior Analytics (UBA) systems detect anomalies in access patterns, such as impossible travel scenarios or sudden access to sensitive systems. These alerts can trigger automatic access restrictions or escalation [53].

Unlike perimeter security, which assumes a binary trusted or untrusted model, identity-based security implements granular and dynamic access controls. Access decisions are made based on real-time evaluation of user context, trust level and resource sensitivity [3].

This model is particularly effective for hybrid and remote work scenarios, where users authenticate from diverse networks, devices and geographic regions. It aligns with modern security principles such as Zero Trust, which mandates continuous verification and least privilege access.

Threat actors have increasingly shifted focus from exploiting infrastructure vulnerabilities to targeting users directly. Phishing, credential stuffing, social engineering and session hijacking are among the most common tactics used to compromise identity. According to Proofpoint [54], more than 80% of reported breaches in the past year involved compromised credentials, highlighting the pivotal role of identity security.

Unlike earlier times when security focused on securing devices or networks, today's attacks target authentication flows, token reuse and improperly configured Single Sign-On (SSO) systems [4]. Attackers leverage legitimate credentials to bypass traditional perimeter defenses, operate under assumed privileges and move laterally within networks undetected. Despite technological advances, human behavior remains one of the weakest links in cybersecurity. Social engineering attacks thrive on user naivety, urgency or emotional manipulation. As such, continuous user education and security awareness training are fundamental components of any identity protection strategy [30]. Effective training programs should focus on:

1) Recognizing phishing and spear-phishing attempts.
2) Safe use of personal devices and public Wi-Fi.
3) Credential management and password hygiene [55].
4) Reporting suspicious emails or access attempts.

Identity in the Context of Zero Trust and NIS2 Identity security is also a foundational element of the ZTA, as defined by NIS2 [28]. ZTA principles dictate that:

1) No user or system is inherently trusted.
2) Access is continually reassessed based on risk and context.
3) Strong identity verification is required at every access point.

The NIS2 Directive from the European Union further reinforces the importance of identity-centric controls. Article 21 of the directive emphasizes access control, identity management and the use of MFA as critical cybersecurity risk management measures for essential and important entities (**Table 4**) [16].

Table 4. Comparative overview—perimeter security vs identity security.

Aspect	Perimeter Security	Identity Security
Security Focus	Network boundaries and corporate infrastructure	Individual user identities and access rights
Trust Model	Implicit trust inside the network	Never trust, always verify
Applicability	Centralized office environments	Hybrid and remote work
Threat Detection	Based on network traffic and firewall rules	Based on user behavior and anomaly detection
Access Control	Static IP-based rules	Dynamic, context-aware policies

Continued

Scalability	Limited to internal infrastructure	Cloud-native, globally scalable
Resilience to Breaches	High impact once perimeter is breached	Compartmentalized access limits lateral movement

As organizations adopt cloud-based services and hybrid work models, identity becomes the most reliable control point for managing access and mitigating threats. Identity security also supports compliance with regulations like the NIS2 Directive, which emphasizes robust identity verification and access controls [16].

To effectively transition to identity security, organizations must implement a coordinated set of technical and cultural changes:

1) Implement enterprise-wide identity governance, including role-based access control and periodic access reviews, to reduce unauthorized access.

2) Enforce MFA and conditional access policies that evaluate device posture, geolocation and risk scoring [4].

3) Audit and minimize privileged accounts through Privileged Access Management (PAM) and just-in-time access provisioning [56].

4) Educating users on phishing and credential hygiene [54].

A hybrid security model that integrates both perimeter and identity controls can offer layered protection. However, in the modern threat landscape, user identity is the new perimeter [57]. Relying solely on network boundaries is no longer viable; robust identity verification is now essential to defend against distributed and persistent cyber threats.

In the context of modern cybersecurity frameworks, user identity security is critical for safeguarding enterprise networks and digital infrastructures. One of the most effective approaches for securing digital identities and preventing unauthorized access is the application of Artificial Intelligence (AI) to detect anomalous user behavior, which may signal compromised credentials, insider threats or identity spoofing.

5.3. The Use of Artificial Intelligence in Detecting Anomalous User Behavior

AI models, particularly those rooted in machine learning (ML) and deep learning (DL), offer the capability to monitor and analyze vast amounts of user activity data in real time. These models learn baseline behavioral profiles based on patterns such as login locations, device usage, access times, application interaction and data movement. When a deviation from the baseline is detected such as unusual access times, atypical device usage or irregular access to sensitive files, the system can trigger alerts or initiate automatic security responses [58].

In identity-centric security architectures, such as Zero Trust, AI plays a central role in continuously validating the legitimacy of users beyond initial authentication. User and Entity Behavior Analytics (UEBA) systems, powered by unsuper-

vised ML algorithms, can identify subtle behavioral anomalies without requiring labeled attack data, making them highly effective in detecting novel or insider threats [59]. For instance, an account used exclusively during work hours on a corporate device may raise suspicion if it is suddenly accessed at night from an unrecognized IP address.

Additionally, supervised learning models such as decision trees, support vector machines (SVM) and neural networks are employed in systems where annotated data is available to train models for identifying risky behavior patterns. Advanced deep learning techniques, including Long Short-Term Memory (LSTM) networks, are particularly effective for modeling temporal sequences of user actions, thus enabling the detection of gradual behavior shifts indicative of evolving threats [60].

The incorporation of AI in identity security has also been enhanced through context-aware authentication systems, where AI evaluates contextual parameters (example: geolocation, biometric inputs, device health) in real time to assess identity legitimacy. These adaptive systems significantly reduce reliance on static credentials, mitigating risks associated with password theft and reuse [61]. Overall, AI-driven detection of anomalous user behavior enhances not only real-time threat visibility but also supports proactive identity threat mitigation, aligning with the principles of continuous authentication and risk-based access control strategies.

However, despite their potential, AI-based cybersecurity systems face notable challenges, including the management of false positives, which can overwhelm security teams and vulnerability to adversarial attacks that deliberately manipulate inputs to deceive machine learning models.

6. Zero Trust Architecture (ZTA)

The evolving cyber threat landscape, driven by cloud migration, remote work and increasingly sophisticated attacks, has rendered traditional perimeter-based security models insufficient. In response, the Zero Trust Architecture (ZTA) has emerged as a foundational security paradigm that aligns with modern enterprise needs. ZTA fundamentally challenges the notion of inherent trust within any network and instead advocates for "never trust, always verify" principles at every access point [62].

According to Abbas *et al.* [62], the implementation of ZTA across various contexts has yielded the following key outcomes:

1) Improved Threat Detection and Prevention—ZTA uses continuous verification mechanisms that significantly minimize the risk of successful attacks. Real-time monitoring and dynamic policy enforcement quickly identify and contain sophisticated threats.

2) Enhanced Access Control—ZTA integrates multi-factor authentication and strict identity verification protocols. This minimizes unauthorized access. Role-based access control and permissions ensure users and devices can only access

necessary resources, reducing the risk of data leaks.

3) Resilience in Distributed Environments—ZTA effectively secures hybrid infrastructures, including cloud environments and remote work setups. Its scalability and adaptability maintain robust security, regardless of system complexity or distribution.

Zero Trust is a comprehensive strategy integrating identity, device, application and network security. According to NIST SP 800-207 [28], the key principles of Zero Trust are:

1) Continuous verification: every access request is dynamically evaluated based on user identity, device health, location, behavior and risk level.

2) Least privilege access: users and devices are granted the minimum level of access necessary to perform their tasks, reducing the potential blast radius of a breach [63].

3) Micro segmentation: networks are broken into small zones with strict controls to prevent lateral movement if one segment is compromised.

4) Assume breach: security systems are designed with the expectation that attackers may already be present within the network, emphasizing detection and rapid response.

6.1. The Implementation of ZTA in Hybrid Environments

Zero Trust is particularly relevant in hybrid work environments, where employees, contractors and partners may access resources from a variety of locations and devices. Effective Zero Trust implementation requires organizations to focus on five foundational pillars [4]:

1) Identity—enforce strong authentication, such as phishing-resistant MFA and continuous identity assurance through anomaly detection.

2) Devices: ensure that endpoints meet security posture requirements (example: OS updates, antivirus, encryption) before granting access.

3) Applications: apply access controls and monitoring for all applications, especially SaaS and legacy systems.

4) Data: classify, label and enforce policies for data access, sharing and encryption.

5) Infrastructure and Networks: use micro segmentation and dynamic access control to contain threats and monitor traffic behavior.

The primary advantages of adopting Zero Trust Architecture in hybrid environments include:

1) Reduces risks from both internal and external threats by eliminating assumptions of implicit trust within the network.

2) Strengthens breach resilience through mechanisms that isolate compromised components and facilitate swift threat detection and response.

3) Facilitates regulatory compliance with frameworks such as GDPR, HIPAA, and the NIS2 Directive by enforcing structured identity and access controls.

4) Enhances visibility and auditability of user access and behavior across the organization's digital infrastructure.

Key obstacles to the successful adoption of ZTA within an enterprise context include:

1) Organizational change: transitioning to ZTA requires cross-departmental alignment, leadership buy-in and cultural adaptation [64].

2) Technical complexity: legacy systems may lack support for ZTA principles or require significant reconfiguration.

3) Cost and resource allocation: ZTA initiatives involve investment in identity platforms, endpoint management, security analytics and staff training.

In a WFH scenario, an employee connects to the corporate network using a personal device that has unknowingly been compromised with malware. In traditional network architecture, this malware could move laterally across the network, potentially accessing file shares, internal applications or even privileged credentials. By contrast, under a Zero Trust Architecture that employs micro-segmentation, the employee's device is restricted to a narrowly defined network segment with access only to essential services. Communication between segments is subject to strict access controls and identity verification. As a result, even if malware is present, it cannot move beyond the isolated segment, effectively containing the threat and preventing it from compromising critical infrastructure or sensitive data. This approach exemplifies the ZTA principle of "never trust, always verify", applied in a dynamic and granular way to modern remote work environments.

6.2. Zero Trust Architecture and Regulatory Compliance (NIS2 Directive)

The integration of ZTA with regulatory compliance frameworks has become increasingly vital, particularly in the context of the EU NIS2 Directive, which came into force in January 2023 (Table 5). As a legal instrument aimed at strengthening the cybersecurity posture of critical and important entities across the European Union, NIS2 significantly raises the bar for both technical and organizational security measures. Its alignment with Zero Trust principles reinforces the necessity for proactive, identity-centric and context-aware security strategies in both public and private sectors [16].

Table 5. Alignment between ZTA and NIS2 directive requirements.

Zero Trust Architecture Principle	Description	Aligned NIS2 Directive Requirement
Identity-First Access Control	Continuous authentication of users and devices before granting access to any resource.	Article 21(2)(b): Access control policies, use of MFA and secure IAM systems
Micro segmentation and Network Isolation	Logical division of the network into secure zones to prevent lateral movement by attackers.	Article 21(2)(d): Measures to ensure protection against unauthorized access and limit breach impact
Real-Time Threat Detection and Response	Integrated monitoring, anomaly detection, and automated responses to minimize attack dwell time.	Article 21(2)(g): Operational continuity, monitoring, and incident response capabilities

7. NIS2 Directive

The NIS2 Directive (Directive (EU) 2022/2555), adopted by the European Parliament and Council in December 2022 and effective from January 2023, represents a significant evolution in the European Union's cybersecurity legislation. It replaces the original NIS Directive (Directive (EU) 2016/1148), aiming to address its shortcomings and adapt to a vastly transformed cyber threat landscape marked by digitalization, interconnectivity and hybrid work environments [65].

NIS2 strengthens the overall level of cybersecurity across the EU by expanding the scope of covered sectors, enhancing risk management obligations, enforcing stricter supervisory measures and introducing harmonized sanctions for non-compliance. It also brings the Directive into closer alignment with contemporary cybersecurity principles such as ZTA.

A key change in NIS2 is the broadened scope of application. The directive applies to both essential (energy, transport, banking, healthcare, digital infrastructure, water, public administration) and important entities (postal services, waste management, food, manufacturing of critical products, digital providers including cloud computing and data centers) in sectors critical to societal and economic functions. Entities are automatically included based on size thresholds (typically > 50 employees or > €10 million turnover) unless otherwise excluded. This approach addresses ambiguity in the original directive, ensuring broader and more consistent application across member states [66]. The research [67] shows that larger small and medium-sized enterprises (SMEs) in telecommunication and energy show moderate preparedness (average score 72.3), while smaller service-based enterprises exhibit lower compliance (average score 48.5). Tikanmäki *et al.* [68] examines hospital cybersecurity and compliance with NIS2 requirements through a specific scenario: "USB infection of a point-of-care testing machine". The study revealed that NIS2 does not specify that the hospitals are forced to have implemented an Intrusion Prevention System (IPS) or Intrusion Prevention Detection System (IDS) in their network.

Under Article 21, all covered entities are required to implement a comprehensive set of technical, operational and organizational security measures, including:

1) Risk analysis and information system security policies.
2) Incident handling and continuity planning.
3) Supply chain security and procurement standards.
4) Access control and identity management.
5) Use of multi-factor authentication and encryption.
6) Employee cybersecurity training.

These measures are outcome-focused and risk-based, allowing flexibility in implementation while establishing clear minimum standards. Importantly, several of these controls directly support and are supported by modern security models like ZTA, which emphasizes identity, least privilege, segmentation and continuous monitoring (**Table 6**) [18].

Table 6. Alignment with ZTA and enterprise security.

NIS2 Measure	ZTA Alignment
Identity and access control policies	Continuous authentication, least privilege, context-aware access
Supply chain security	Trust boundaries, third-party identity assurance
Incident detection and response	Real-time monitoring, automated containment and response
Risk-based governance	Adaptive policy enforcement, continuous evaluation of trust

8. Discussions

The transition from traditional office-based work to hybrid and fully remote models has fundamentally altered the cybersecurity threat landscape. The COVID-19 pandemic accelerated this shift, forcing organizations to rapidly adopt digital solutions and remote connectivity, often without sufficient time to adapt their security architecture. As a result, legacy perimeter-based defenses have shown critical limitations, especially in the face of increasingly sophisticated attacks targeting user credentials, remote access points and cloud services.

The analysis in this article demonstrates that WFO environments, while benefiting from centralized IT control and network segmentation, often foster a false sense of security. On the other hand, remote work environments introduce unique vulnerabilities such as unmanaged personal devices, unsecured home networks and reduced visibility into user behavior. These changes emphasize the growing importance of identity as the new perimeter, shifting the focus from location-based access to context and identity-based controls.

The emergence of ZTA is a direct response to these evolving threats. ZTA's emphasis on continuous verification, least-privilege access and micro segmentation aligns well with the dynamic nature of hybrid work environments. Its adoption helps mitigate both insider and outsider threat and enhances organizational resilience by minimizing lateral movement during a breach. However, implementing ZTA presents operational challenges, including integration with legacy systems, the need for comprehensive identity governance and significant cultural and technical shifts within organizations.

Describing ZTA adoption as a "cultural shift" reflects the broader transformation required in organizational mindset and behavior, as outlined in NIST SP 800-207. Zero Trust moves away from the traditional assumption of implicit trust within network boundaries toward a model of continuous, explicit verification based on identity, device posture and contextual risk. This shift affects not only technical architecture but also organizational policies and practices. Employees and leadership alike must adopt a posture of 'never trust, always verify,' which has direct implications for security awareness training, emphasizing concepts such as least privilege, segmentation and dynamic access control. From a policy stand-

point, organizations must implement adaptive access management, continuous monitoring and risk-based authentication as core elements of their cybersecurity posture. Effective change management is critical to this transition and should include executive leadership endorsement, alignment with NIST Cybersecurity Framework (CSF) functions, particularly Identify, Protect and Respond, and structured communication and training plans. Without integrating these cultural and procedural dimensions, organizations risk falling short of the full security benefits envisioned in a Zero Trust model.

Moreover, regulatory frameworks such as the NIS2 Directive reinforce the relevance of ZTA by mandating robust cybersecurity measures that directly overlap with Zero Trust principles. Organizations subject to NIS2 must adopt practices such as MFA, risk-based access controls, supply chain risk management and real-time threat monitoring. This convergence between regulatory compliance and architectural best practices provides an opportunity for companies to unify their security strategy under a single, scalable and auditable framework.

Despite these advancements, several areas warrant further discussion:

1) User Behavior and Awareness: both office and remote environments remain vulnerable to social engineering and phishing attacks. The human factor remains a critical weakness, underscoring the need for continuous security awareness and training programs.

2) Technology Gaps and Vendor Lock-in: the successful implementation of ZTA requires the integration of multiple technologies (example: IAM, Security Information and Event Management (SIEM), Software-Defined Perimeter (SDP)). Without proper planning, organizations risk fragmentation or over-reliance on specific vendors.

3) Regulatory Ambiguity and Interoperability: while NIS2 offers a strong baseline, its practical interpretation and enforcement vary across EU member states. This may pose challenges for multinational organizations operating under multiple legal jurisdictions.

4) Scalability and Cost: especially for SMEs, the financial and technical burden of transitioning to ZTA or complying with NIS2 may be significant. Risk-based prioritization and phased implementation are essential to achieving progress without overwhelming resources.

The security paradigm must continue to evolve beyond physical boundaries and static defenses. A layered, identity-centric approach, grounded in ZT and aligned with regulatory mandates like NIS2, offers the most effective path forward for securing both office-based and remote work environments. However, its success depends not only on technology, but also on organizational leadership, cross-functional collaboration and ongoing investment in cybersecurity maturity.

9. Conclusion

The objective of this review is to provide a comprehensive and unified source of information for scientists, engineers, researchers and organizations engaged in the

investigation of recent advancements and challenges associated with the concepts of work from home and work from office. The COVID-19 pandemic significantly reshaped how and where we work, triggering a rapid shift to remote operations and exposing both new and existing cybersecurity vulnerabilities. While WFO environments faced intensified threats like ransomware and insider risks, the rise of WFH brought a surge in phishing, weak network defenses and unregulated use of personal and third-party tools. This evolving threat landscape underscores the urgent need for organizations to adopt adaptive, risk-based cybersecurity strategies that extend beyond the traditional perimeter. Proactive measures such as regular security training, multi-factor authentication, secure remote access solutions and continuous risk assessments, are essential in building resilience for both office-based and remote work models. As work environments continue to evolve post-pandemic, maintaining cybersecurity must remain a shared responsibility between organizations and employees to safeguard data, infrastructure and trust in the digital workspace.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Choudhury, P., Foroughi, C. and Larson, B. (2020) Work-From-Anywhere: The Productivity Effects of Geographic Flexibility. *Strategic Management Journal*, **42**, 655-683. https://doi.org/10.1002/smj.3251

[2] Brynjolfsson, E., Horton, J.J., Ozimek, A., Rock, D., Sharma, G. and TuYe, H.Y. (2020) COVID-19 and Remote Work: An Early Look at US Data (No. w27344). National Bureau of Economic Research.

[3] Kindervag, J. and Balaouras, S. (2010) No More Chewy Centers: Introducing the Zero Trust Model of Information Security. *Forrester Research*, **3**, 1-16.

[4] Microsoft (2021) Zero Trust Deployment Guide for Microsoft 365. https://docs.microsoft.com

[5] Ahmad, T. (2020) Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3568830

[6] Kotak, J., Habler, E., Brodt, O., Shabtai, A. and Elovici, Y. (2023) Information Security Threats and Working from Home Culture: Taxonomy, Risk Assessment and Solutions. *Sensors*, **23**, Article 4018. https://doi.org/10.3390/s23084018

[7] Borkovich, D.J. and Skovira, R.J. (2020) Working from Home: Cybersecurity in the Age of COVID-19. *Issues in Information Systems*, **21**, 234-236.

[8] Venkatesha, S., Reddy, K.R. and Chandavarkar, B.R. (2021) Social Engineering Attacks during the COVID-19 Pandemic. *SN Computer Science*, **2**, Article No. 78. https://doi.org/10.1007/s42979-020-00443-1

[9] Granneman, J. (2021) Working from Home: A Hacker's Perspective. *The Journal of Equipment Lease Financing* (*Online*), **39**, 1-10.

[10] Adame, D. (2021) Managing and Securing Endpoints: A Solution for a Telework Environment. Ph.D. Thesis, California State University.

[11] Ribeiro, S. (2021) Remote Work and Data Protection: How do Organisations Secure Personal Data Protection Compliance from Home? *Bobcatsss*, 246-255. https://doi.org/10.34630/bobcatsss.vi.4983

[12] Khan, Z. and Charan, P. (2023) Work-From-Home Security Issues and Risk over Internet. *Sustainable Environment, Manifestation and Augmentation*, **1**, 468-472.

[13] Hui, K., Kim, S.H. and Wang, Q. (2017) Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly*, **41**, 497-523. https://doi.org/10.25300/misq/2017/41.2.08

[14] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003) The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, **11**, 431-448. https://doi.org/10.3233/jcs-2003-11308

[15] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) Increasing Cybersecurity Investments in Private Sector Firms. *Journal of Cybersecurity*, **1**, 3-17. https://doi.org/10.1093/cybsec/tyv011

[16] European Union Agency for Cybersecurity (ENISA) (2023) Guidelines on the Implementation of the NIS2 Directive. https://www.enisa.europa.eu/

[17] Cao, Y., Pokhrel, S.R., Zhu, Y., Doss, R. and Li, G. (2024) Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges. *Machine Intelligence Research*, **21**, 294-317. https://doi.org/10.1007/s11633-023-1456-2

[18] Emmanni, P.S. (2024) Implementing a Zero Trust Architecture in Hybrid Cloud Environments. *International Journal of Computer Trends and Technology*, **72**, 33-39. https://doi.org/10.14445/22312803/ijctt-v72i5p104

[19] Ojo, A.O. (2025) Adoption of Zero Trust Architecture (ZTA) in the Protection of Critical Infrastructure. *Path of Science*, **11**, 5001-5009. https://doi.org/10.22178/pos.113-2

[20] Vandezande, N. (2024) Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor. *Computer Law & Security Review*, **52**, Article ID: 105890. https://doi.org/10.1016/j.clsr.2023.105890

[21] Bowo, A., Hakkala, A. and Sainio, P. (2025) Adapting Cybersecurity Frameworks for NIS2 Compliance. Ph.D. Thesis, University of Turku.

[22] Ferrier, E. (2024) LibGuides: Guide to Searching: Citation Searching. https://libguides.brown.edu/searching/citation

[23] Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., *et al.* (2015) Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols (PRISMA-P) 2015 Statement. *Systematic Reviews*, **4**, Article No. 1. https://doi.org/10.1186/2046-4053-4-1

[24] Shinder, D.L. and Cross, M. (2008) Scene of the Crime: Computer Forensics Handbook. Syngress Publishing.

[25] Ali, M., Khan, S.U. and Vasilakos, A.V. (2015) Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, **305**, 357-383. https://doi.org/10.1016/j.ins.2015.01.025

[26] Federal Bureau of Investigation (FBI) (2020) Cybercrime Reports Spike during COVID-19 Pandemic. https://www.fbi.gov/

[27] Posey, C. and Shoss, M. (2023) Employees as a Source of Security Issues in Times of Change and Stress: A Longitudinal Examination of Employees' Security Violations during the COVID-19 Pandemic. *Journal of Business and Psychology*, **39**, 1027-1048. https://doi.org/10.1007/s10869-023-09917-4

[28] National Institute of Standards and Technology (NIST) (2020) Special Publication 800-207: Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207

[29] Greitzer, F.L. and Frincke, D.A. (2010) Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In: Probst, C., Hunker, J., Gollmann, D. and Bishop, M., Eds., *Insider Threats in Cyber Security*, Springer, 85-113. https://doi.org/10.1007/978-1-4419-7133-3_5

[30] SANS Institute (2020) Lateral Movement: Detecting and Responding to In-Network Threats. https://www.sans.org

[31] Dolci, P.C. and Maçada, A.C. (2022) A Model to Understand Digital Capabilities, Shadow IT and Individual Performance in the Context of Remote Work. https://aisel.aisnet.org/confirm2022/2/

[32] Slavković, M., Sretenović, S. and Bugarčić, M. (2021) Remote Working for Sustainability of Organization during the COVID-19 Pandemic: The Mediator-Moderator Role of Social Support. *Sustainability*, **14**, Article 70. https://doi.org/10.3390/su14010070

[33] Wilcox, H. and Bhattacharya, M. (2020) A Human Dimension of Hacking: Social Engineering through Social Media. *IOP Conference Series*: *Materials Science and Engineering*, **790**, Article ID: 012040. https://doi.org/10.1088/1757-899x/790/1/012040

[34] Sundar, K. and Kumar, S. (2016) Blue Screen of Death Observed for Microsoft Windows Server 2012 R2 under DDoS Security Attack. *Journal of Information Security*, **7**, 225-231. https://doi.org/10.4236/jis.2016.74018

[35] Zhu, L., Li, J. and Bai, L. (2022) The Influence of Network Public Opinion on Audit Credibility: A Dynamic Rumor Propagation Model Based on User Weight. *Information*, **13**, Article 90. https://doi.org/10.3390/info13020090

[36] Mahyoub, M., Matrawy, A., Isleem, K. and Ibitoye, O. (2025) Cybersecurity Challenge Analysis of Work-From-Anywhere (WFA) and Recommendations Guided by a User Study. *IEEE Transactions on Human-Machine Systems*, **55**, 428-439. https://doi.org/10.1109/thms.2025.3552231

[37] Nurse, J.R.C., Williams, N., Collins, E., Panteli, N., Blythe, J. and Koppelman, B. (2021) Remote Working Pre- and Post-Covid-19: An Analysis of New Threats and Risks to Security and Privacy. In: Stephanidis, C., Antona, M. and Ntoa, S., Eds., *HCI International* 2021—*Posters*, Springer, 583-590. https://doi.org/10.1007/978-3-030-78645-8_74

[38] Ahsan Pritom, M.M., Schweitzer, K.M., Bateman, R.M., Xu, M. and Xu, S. (2020) Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses. 2020 *IEEE International Conference on Intelligence and Security Informatics* (*ISI*), Arlington, 9-10 November 2020, 1-6. https://doi.org/10.1109/isi49825.2020.9280539

[39] Rajkumar, P.V., Raghavan, K. and Desai, M. (2023) Cyber Security and Hybrid Work Environments. *SAM Advanced Management Journal*, **88**, 44-55.

[40] Sabin, J. (2021) The Future of Security in a Remote-Work Environment. *Network Security*, **2021**, 15-17. https://doi.org/10.1016/s1353-4858(21)00118-5

[41] Whitty, M.T., Moustafa, N. and Grobler, M. (2024) Cybersecurity When Working from Home during COVID-19: Considering the Human Factors. *Journal of Cybersecurity*, **10**, tyae001. https://doi.org/10.1093/cybsec/tyae001

[42] Yang, J. and Linkeschova, L. (2021) Remote Working and Cybersecurity in the Pandemic. https://access.archive-ouverte.unige.ch/access/metadata/275c55aa-49b0-40c6-8bfd-edad32e29ef0/download

[43] Rawal, B.S., Manogaran, G. and Peter, A. (2023) Cybersecurity and Identity Access Management. Springer

[44] Süß, R. and Süß, Y. (2024) Data Center Security and Resiliency. In: Süß, R. and Süß, Y., Eds., *IT Infrastructure*, Apress, 203-234. https://doi.org/10.1007/979-8-8688-0077-1_7

[45] Bolding, D. (1995) Network Security, Filters and Firewalls. *XRDS*: *Crossroads*, *The ACM Magazine for Students*, **2**, 8-10. https://doi.org/10.1145/332198.332205

[46] Vemula, S., Gooley, J. and Hasan, R. (2020) Cisco Software-Defined Access. Cisco Press.

[47] Almadani, M.S., Alotaibi, S., Alsobhi, H., Hussain, O.K. and Hussain, F.K. (2023) Blockchain-based Multi-Factor Authentication: A Systematic Literature Review. *Internet of Things*, **23**, Article ID: 100844. https://doi.org/10.1016/j.iot.2023.100844

[48] Pandey, P. and Nisha, T.N. (2021) Challenges in Single Sign-On. *Journal of Physics*: *Conference Series*, **1964**, Article ID: 042016. https://doi.org/10.1088/1742-6596/1964/4/042016

[49] Kuokkanen, A. (2020) Newcomer's introduction to Privileged Access Management. https://www.theseus.fi/bitstream/handle/10024/348503/Opinnaytetyo_Kuokkanen_Antti.pdf?sequence=2

[50] Okta (2023) IAM for the Hybrid Workforce. https://www.okta.com

[51] Alshehri, A., Khan, N., Alowayr, A. and Yahya Alghamdi, M. (2023) Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics. *Computer Systems Science and Engineering*, **44**, 1679-1689. https://doi.org/10.32604/csse.2023.026526

[52] Ganiyu, S.O. and Jimoh, R.G. (2021) Extended Risk-Based Context-Aware Model for Dynamic Access Control in Bring Your Own Device Strategy. In: Chiroma, H., Abdulhamid, S.M., Fournier-Viger, P. and Garcia, N.M., Eds., *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics*, Springer, 295-315. https://doi.org/10.1007/978-3-030-66288-2_12

[53] CrowdStrike (2023) Identity Protection with UBA and EDR Integration. https://www.crowdstrike.com

[54] 55 Proofpoint (2022) State of the Phish Report. https://www.proofpoint.com

[55] Benantar, M. (2005) Access Control Systems: Security, Identity Management and Trust Models. Springer Science & Business Media.

[56] CyberArk (2023) Privileged Access Management: Security for High-Risk Accounts. https://www.cyberark.com

[57] Zscaler (2022) ThreatLabz Report: Lateral Movement in Cloud Environments. https://www.zscaler.com

[58] Veeramachaneni, K., Arnaldo, I., Korrapati, V., Bassias, C. and Li, K. (2016) AI^2: Training a Big Data Machine to Defend. 2016 *IEEE 2nd International Conference on Big Data Security on Cloud* (*BigDataSecurity*), *IEEE International Conference on High Performance and Smart Computing* (*HPSC*), *and IEEE International Conference on Intelligent Data and Security* (*IDS*), New York, 9-10 April 2016, 49-52. https://doi.org/10.1109/bigdatasecurity-hpsc-ids.2016.79

[59] Liang, Y., Samtani, S., Guo, B. and Yu, Z. (2020) Behavioral Biometrics for Continuous Authentication in the Internet-Of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet of Things Journal*, **7**, 9128-9143. https://doi.org/10.1109/jiot.2020.3004077

[60] Sharma, B., Pokharel, P. and Joshi, B. (2020) User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder—Insider Threat Detection. *Proceedings of the 11th International Conference on Advances in Information Technology*, Bangkok, 1-3 July 2020, 1-9. https://doi.org/10.1145/3406601.3406610

[61] Glöckler, J., Sedlmeir, J., Frank, M. and Fridgen, G. (2023) A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Business & Information Systems Engineering*, **66**, 421-440. https://doi.org/10.1007/s12599-023-00830-x

[62] Abbas, G. and Gul, S. (2025) Zero Trust Architecture: Revolutionizing Cybersecurity in the Era of Advanced Threats. *International Journal of Management, Technology and Engineering*, XIV.

[63] Mickie, J. and Weng, J. (2025) Zero Trust Security: A Proactive Cybersecurity Model for Risk Management. https://www.researchgate.net/profile/Jiefeng-Weng/publication/388848722_Zero_Trust_Security_A_Proactive_Cybersecurity_Model_for_Risk_Management/links/67aa1ede645ef274a479b0f0/Zero-Trust-Security-A-Proactive-Cybersecurity-Model-for-Risk-Management.pdf?__cf_chl_tk=Mqpgw2lbGQzyj5qbMa-bOLxzZbDwTHwnm9wvpzUddEOc-1755002182-1.0.1.1-VqgkeEmhORwSHDD-wUfDbF3DPXO2qa0K1alb110c.lWc

[64] Yuryna Connolly, L., Lang, M., Gathegi, J. and Tygar, D.J. (2017) Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Study. *Information & Computer Security*, **25**, 118-136. https://doi.org/10.1108/ics-03-2017-0013

[65] Gaie, C. and Mueck, M. (2025) Introduction to the Networks and Information Systems 2 (NIS2) Directive. In: Mueck, M. and Gaie, C., Eds., *European Digital Regulations*, Springer, 161-180. https://doi.org/10.1007/978-3-031-80809-8_7

[66] European Commission (2022) Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2). https://eur-lex.europa.eu

[67] Joswig, T. and Kurz, W. (2025) Empirical Analysis of NIS2 Adoption in EU Smes: Challenges for Critical Infrastructure in Germany. *Journal of Next-Generation Research* 5.0, **1**, 1-21. https://doi.org/10.70792/jngr5.0.v1i3.99

[68] Tikanmäki, I., Rajamäki, J., Boateng, F., Kaikkonen, J., Ketene, B., Lehtiaho, J., *et al.* (2025) Cyber Threats in Hospitals: GDPR and NIS2 Regulations in Preventing USB Injections. *International Conference on Cyber Warfare and Security*, **20**, 461-468. https://doi.org/10.34190/iccws.20.1.3308