



American Journal of Education and Technology (AJET)

ISSN: 2832-9481 (ONLINE)

VOLUME 5 ISSUE 4 (2026)



PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

Applying Security-by-Design Principles in Next-Generation Network Architectures: Implications for the United States and Global Cybersecurity Ecosystems

Akeem Ogundipe*

Article Information

Received: May 01, 2026

Accepted: August 06, 2026

Published: October 01, 2026

Keywords

5G Networks, Cloud Security, Cybersecurity Policy, Edge Computing, ENISA Guidelines, Global Security Frameworks, ISO/IEC 27001, Network Security, NIST Framework, Secure Network Architecture, Security-By-Design, Zero Trust Architecture

ABSTRACT

The rapid growth of the digital ecosystem—driven by technologies such as 5G, cloud-native systems, edge computing, and the Internet of Things (IoT)—has introduced both significant opportunities and complex cybersecurity challenges. As modern networks become increasingly interconnected, traditional reactive security approaches are proving inadequate against evolving and sophisticated cyber threats. In this context, Security-by-Design (SbD) has emerged as a proactive approach that embeds security considerations into system architecture and throughout the development lifecycle.

This study examines the implementation of Security-by-Design principles in the United States and compares them with practices across Europe, the Asia-Pacific region, and Africa. The analysis draws on a combination of academic literature, policy documents, and established security frameworks, including NIST SP 800-207, CISA's Zero Trust initiatives, ENISA guidelines, and ISO/IEC 27001 standards.

The findings indicate that the United States leads in aligning Zero Trust architecture with Security-by-Design principles, largely supported by federal mandates and national cybersecurity strategies. In contrast, other regions demonstrate strong governance frameworks, enhanced data protection regulations, and context-specific technological adaptations. The paper concludes by identifying ongoing global challenges, outlining future research directions, and recommending strategies to improve international collaboration in securing next-generation network infrastructures.

INTRODUCTION

The rapid pace of digital transformation has increased the need for secure, reliable, and scalable network systems. Technologies such as 5G, cloud computing, edge computing, and the Internet of Things (IoT) are changing how systems connect and operate, but they also introduce new security risks. As cyber threats become more advanced, traditional security approaches that rely mainly on perimeter defenses are no longer enough. This has brought renewed attention to Security-by-Design (SbD), which focuses on building security into systems from the very beginning rather than adding it later.

In the United States, this approach is reflected in national cybersecurity efforts such as Executive Order 14028, NIST's Zero Trust Architecture guidelines, and CISA's Secure-by-Design initiative. Similar ideas appear in global frameworks like ISO/IEC 27001, GDPR, and ENISA guidelines, although the level of adoption differs across regions due to variations in policy, resources, and technological development.

This study explores how Security-by-Design is applied in next-generation network architectures in the United States and compares it with practices in other regions, including Europe, Asia-Pacific, Africa, and Latin America. It also examines key challenges and identifies opportunities for stronger global collaboration in cybersecurity.

LITERATURE REVIEW

Existing research in cybersecurity consistently emphasizes

the need to embed security principles directly into system design, policy development, and enterprise architecture. Early studies focused largely on the theoretical foundations of secure systems, while more recent work has expanded into practical applications across cloud computing, distributed networks, and Zero Trust environments. Across regions, cybersecurity frameworks often reflect different priorities—for example, privacy-driven approaches in Europe, modernization-focused strategies in the United States, and sovereignty-oriented policies in parts of Asia. This section brings together both foundational ideas and recent studies that shape current Security-by-Design (SbD) practices, particularly in cloud systems, Zero Trust architectures, and global regulatory environments.

Conceptual Foundations of Security-by-Design

The idea of Security-by-Design can be traced back to the foundational work of Jerome H. Saltzer and Michael D. Schroeder (1975), who introduced key principles such as least privilege, complete mediation, and fail-safe defaults. These principles emphasized that security should be built into systems from the outset rather than added as an afterthought. Over time, these ideas have remained central to modern cybersecurity practices.

In recent years, Security-by-Design has evolved from a theoretical concept into a practical framework embedded within secure software development lifecycles and enterprise governance. This includes integrating

¹ 5230 S M L King Jr Pkwy, Beaumont, TX 77705, Lamar University, United States

* Corresponding author's e-mail: keemgundipe@gmail.com

security considerations from the early stages of system design through deployment and ongoing maintenance. Activities such as risk assessment, threat modeling, secure coding, automated testing, and continuous monitoring are now widely recognized as essential components of this approach. As digital systems continue to grow in complexity, embedding security early has become a necessary step toward building resilient infrastructures. Recent studies in the American Journal of Education and Technology also reinforce this perspective. For example, Fazil *et al.* (2023) highlight how gaps in cybersecurity awareness can expose users and systems to significant risks, emphasizing the importance of integrating security principles not only at the technical level but also in user interaction and system design.

Security-by-Design in Cloud and Distributed Environments

Cloud computing environments—whether public, private, or hybrid—are inherently dynamic and require security to be embedded directly into their architecture. Security-by-Design in cloud systems focuses on principles such as identity-based access control, least-privilege enforcement, API security, and continuous configuration monitoring. These practices help organizations manage risks associated with scalability, shared infrastructure, and remote access.

In the United States, initiatives such as FedRAMP promote Security-by-Design by enforcing standardized security controls and continuous monitoring requirements across cloud services. Globally, standards such as ISO/IEC 27017 and ISO/IEC 27018 extend similar principles to cloud-specific environments. European frameworks, particularly under GDPR, emphasize privacy-by-design, while countries in the Asia-Pacific region often align security practices with national security and data sovereignty goals.

The growing reliance on digital platforms across sectors further highlights the importance of integrating security into system design. Gonzalo (2024), in the American Journal of Education and Technology, notes that digital transformation—driven by technologies such as cloud computing, IoT, and artificial intelligence—has increased both operational efficiency and exposure to cybersecurity risks. This reinforces the need for proactive security strategies that are embedded from the early stages of system development.

Security-by-Design and Zero Trust Architecture

Zero Trust Architecture (ZTA) represents one of the most practical implementations of Security-by-Design. Built on the principle of “never trust, always verify,” Zero Trust requires continuous authentication, strict access control, and network segmentation. The NIST SP 800-207 framework provides a widely accepted model for implementing these principles, ensuring that security is enforced across all layers of a system.

Regional approaches to Zero Trust vary. In Europe,

ENISA guidelines emphasize privacy, data protection, and compliance with regulatory frameworks such as GDPR, often focusing on data minimization and privacy-preserving access controls. In contrast, the United States has driven Zero Trust adoption through federal cybersecurity modernization efforts and the need to secure large-scale government systems.

Despite these differences, the core idea remains consistent: security must be embedded into the architecture and operation of systems rather than applied as an external layer. This alignment between Zero Trust and Security-by-Design highlights a broader shift in cybersecurity thinking—from reactive defense mechanisms to proactive, design-centered strategies.

Global Perspectives: EU, Asia-Pacific, Africa, and Latin America

Security-by-Design (SbD) is gaining attention worldwide, but how it is applied differs across regions.

European Union

The European Union stands out as one of the most highly regulated environments. Frameworks such as GDPR, NIS2, and guidance from ENISA place strong emphasis on privacy-by-design, requiring organizations to build privacy and security controls into systems from the earliest stages of development. This approach reflects the EU’s broader focus on data protection and user rights.

Asia-Pacific

Several countries in the Asia-Pacific region—including Japan, South Korea, Singapore, and Australia—are actively advancing SbD through national cybersecurity strategies and cloud security initiatives. In many cases, these efforts are supported by government-led programs and regulatory guidance. While some countries apply SbD broadly, others focus more on critical sectors such as infrastructure, IoT, and industrial systems.

Africa

In Africa, countries like Nigeria, Kenya, and South Africa are gradually incorporating SbD into their digital transformation efforts. Although progress is evident, challenges such as limited resources, skills gaps, and legacy systems continue to slow widespread adoption. Even so, there is growing alignment with international standards, particularly ISO-based frameworks.

Latin America

Across Latin America, adoption levels vary significantly. Some countries have made notable progress by integrating SbD into cloud governance and data protection laws, while others face delays due to uneven regulatory frameworks and economic constraints. Despite these differences, interest in SbD continues to grow across the region.

Overall, while Security-by-Design is becoming a global priority, the extent of its implementation is closely shaped

by each region's regulatory environment, economic capacity, and level of technological development.

Theoretical Framework

This study is grounded in three related concepts that help explain how Security-by-Design (SbD) can be effectively integrated into modern digital systems.

Zero Trust Architecture (ZTA)

Zero Trust Architecture serves as the central framework for this study. Instead of assuming that users or systems inside a network can be trusted, Zero Trust requires continuous verification. Its core ideas—such as verifying every request, limiting access to only what is necessary, and assuming that breaches can occur—closely align with the principles of Security-by-Design. In practice, this means building systems that rely on identity-based controls, continuous authentication, and network segmentation from the start. Rather than adding security later, Zero Trust encourages organizations to design systems where access control, multi-factor authentication, and policy enforcement are part of the foundation.

Risk Management Framework (RMF)

The second foundation comes from risk management approaches, particularly the NIST Risk Management Framework and ISO/IEC 27005. These frameworks provide a structured way to identify risks, select appropriate controls, and continuously monitor systems over time. Within the context of Security-by-Design, they help ensure that security decisions are guided by risk from the early stages of development. Practices such as threat modeling and impact assessment become essential tools, allowing organizations to design systems that reflect their specific risk environment rather than applying generic security measures.

Systems Engineering Perspective

The third perspective is drawn from systems engineering, which focuses on designing and managing complex, interconnected systems. This approach highlights the importance of considering the entire system—including hardware, software, users, and processes—as a unified whole. Concepts such as modular design, reliability, redundancy, and lifecycle management are especially relevant here. From this viewpoint, Security-by-Design

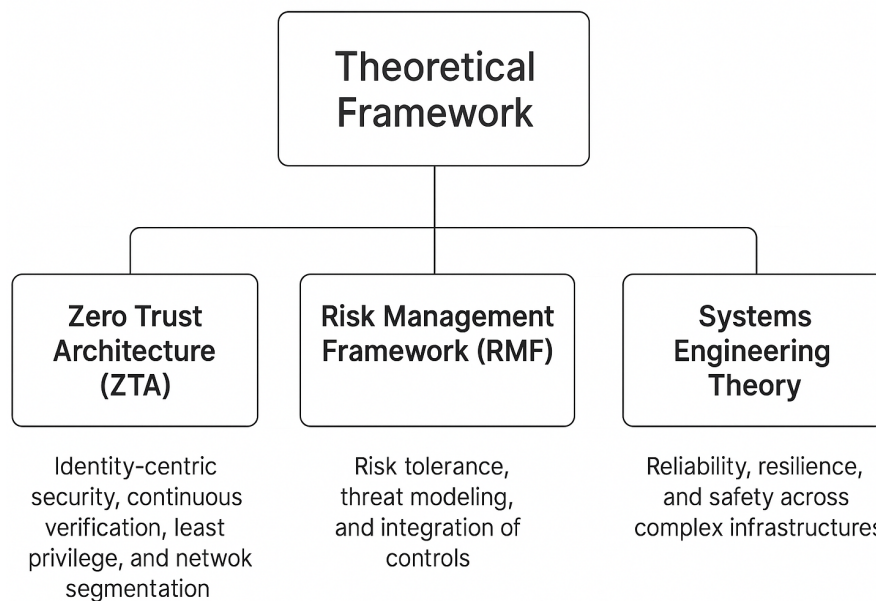


Figure 1: Theoretical Framework Integrating Zero Trust Architecture, Risk Management Framework, and Systems Engineering Theory.

is not just about adding technical controls but about ensuring that security is built into the system at every stage, supporting long-term resilience and continuous operation.

The theoretical framework diagram illustrates how this study brings together three complementary perspectives to examine Security-by-Design practices. Zero Trust Architecture provides the core principle of “never trust, always verify,” emphasizing continuous validation of access and identity. The Risk Management Framework offers a structured approach to identifying threats and aligning security controls with an organization's risk

tolerance. At the same time, a systems engineering perspective ensures that security is considered across the entire system, supporting resilience in complex and interconnected environments. Taken together, these perspectives provide a unified lens for understanding and evaluating modern cybersecurity architectures.

MATERIALS AND METHODS

This study adopts a conceptual and qualitative research design to explore how Security-by-Design principles are understood and applied across different regions. A qualitative approach is used to provide deeper insight,

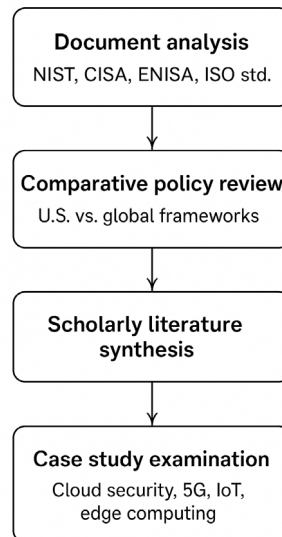


Figure 2: Qualitative Methodology Workflow for the Study

strengthen the analysis, and support meaningful comparisons.

The methodology diagram outlines a staged qualitative approach that guides the analysis in this study. It brings together several methods—document analysis, comparative policy review, literature synthesis, and case study examination—into a single, coherent workflow. This structure helps ensure that the analysis is both systematic and well-integrated across different sources of evidence.

Document Analysis

In this study, key cybersecurity standards and guidance documents, including those developed by NIST, CISA, ENISA, and the ISO/IEC series—were systematically reviewed. The goal was to identify common security principles, highlight differences in regulatory focus, and track evolving best practices, particularly in areas such as access control, Zero Trust, and Security-by-Design. This document analysis provides a strong conceptual foundation, grounded in widely recognized and established frameworks.

Comparative Policy Review

This study also includes a structured comparison of cybersecurity frameworks in the United States and other regions, including the EU, the U.K., Asia-Pacific, Africa, and Latin America. It examines how differences in legal systems, cultural contexts, and regulatory environments influence the adoption of Security-by-Design. The comparative analysis highlights region-specific priorities—such as privacy in the EU and cyber sovereignty in parts of Asia-Pacific—and shows how these differences shape the way SbD is implemented across regions.

Scholarly Literature Synthesis

This study draws on a range of peer-reviewed articles, books, and technical reports to capture both the

theoretical development and practical application of Security-by-Design. The literature covers key areas such as cloud security, Zero Trust architecture, identity governance, and secure systems engineering. By bringing these sources together, the review supports the study's conceptual framework and ensures it is grounded in current academic and professional discussions.

Case Study Examination

The study includes a set of illustrative case studies drawn from areas such as cloud security, 5G networks, IoT environments, and edge computing. These examples help show how Security-by-Design works in real-world settings. They highlight practical challenges—including scalability, interoperability, and integration with legacy systems—while also demonstrating successful applications of principles like least privilege and Zero Trust controls.

Overall Contribution of the Methodology

Together, these qualitative approaches provide a detailed and well-rounded understanding of how Security-by-Design is applied in modern cybersecurity architectures. The methodology captures regional differences, highlights the influence of policy and regulation, and connects theoretical concepts with real-world technological environments. By combining these perspectives, the study offers a more balanced and comprehensive view of how SbD is implemented across different contexts, strengthening the overall depth and reliability of the analysis.

RESULTS AND DISCUSSION

Security-by-Design in U.S. Next-Generation Networks

The United States has positioned itself as a global leader in implementing Security-by-Design (SbD), embedding it into federal policies, technical standards, and the development of next-generation digital systems. This

reflects a clear national priority: strengthening the resilience of critical sectors against evolving cyber threats linked to cloud computing, 5G, and industrial technologies. In the U.S., SbD is not just a theoretical idea—it is treated as a practical requirement, supported by executive directives and well-established cybersecurity frameworks. The overall approach emphasizes prevention, continuous verification, and integrating security into systems from the earliest stages of design.

Federal Mandates

Federal policies play a key role in driving the adoption of Security-by-Design across government agencies and critical infrastructure. A major example is Executive Order 14028, introduced in 2021, which accelerated efforts to improve national cybersecurity. The order requires federal agencies to strengthen software supply chain security, adopt Zero Trust principles, and modernize outdated systems. It also places responsibility on vendors and service providers to build secure systems that align with these expectations.

In addition, the Cybersecurity and Infrastructure Security Agency (CISA) has promoted a Secure-by-Design approach that shifts responsibility toward software developers and technology providers. Rather than relying on end users to configure security correctly, this initiative encourages vendors to deliver products with secure default settings, built-in protections, and continuous security testing throughout the product lifecycle. Together, these efforts position SbD as a measurable and enforceable component of U.S. cybersecurity strategy.

NIST Frameworks

The National Institute of Standards and Technology (NIST) provides the technical foundation for implementing Security-by-Design in the United States. Its frameworks are widely used across both government and industry to guide secure system development.

Key NIST publications include

- NIST SP 800-207 (Zero Trust Architecture): This framework outlines a model based on continuous verification, strict access control, and identity-focused security. It eliminates the idea of implicit trust within networks and aligns closely with SbD principles by ensuring security is built into system operations.
- NIST SP 800-53 (Security and Privacy Controls): This standard defines a comprehensive set of controls—technical, operational, and managerial—that must be integrated into information systems. It reinforces the idea that security should be embedded at every layer of system design.
- NIST SP 800-160 (Systems Security Engineering): This publication takes a systems engineering approach, emphasizing the integration of security throughout the entire system lifecycle. It supports SbD by focusing on resilience, fault tolerance, and secure architecture design. Together, these frameworks form the backbone of Security-by-Design practices in the United States,

providing both conceptual guidance and practical tools for building secure and resilient systems.

Technological Domains

Security-by-Design (SbD) is applied across several technological domains in the United States, each with its own architectural considerations and security challenges. While the core principles remain consistent, their implementation varies depending on the nature of the technology.

5G Networks

In U.S. 5G deployments, SbD is closely tied to technologies such as virtualization, software-defined networking (SDN), and network slicing. These features allow for more flexible network management, including dynamic segmentation and isolation, which help reduce potential attack surfaces. There is also a strong focus on securing the supply chain and integrating Zero Trust principles into both core and edge components of 5G infrastructure. This ensures that security is maintained even as networks become more distributed and complex.

Cloud-Native Systems

Cloud security in the United States is largely guided by frameworks such as FedRAMP, which enforces strict Security-by-Design requirements for federal cloud service providers. These include continuous monitoring, identity-based access control, and the use of Zero Trust principles across multi-cloud and hybrid environments. In practice, SbD is reflected in areas such as API security, workload isolation, and automated compliance processes, all of which help maintain consistent security across dynamic cloud systems.

Critical Infrastructure

In the United States, critical sectors such as energy, transportation, manufacturing, and healthcare apply Security-by-Design (SbD) through frameworks tailored to Industrial Control Systems (ICS) and Operational Technology (OT). These approaches emphasize secure system architecture, network segmentation between IT and OT environments, least-privilege access, continuous monitoring, and resilience planning. Together, these measures help reduce risks at a national level.

More broadly, SbD in the U.S. is supported by a combination of regulatory enforcement, technical standards, and ongoing modernization efforts across sectors. There is a strong focus on scalability, automation, supply chain security, and real-time threat detection. Compared to other regions, the U.S. approach stands out for its rapid adoption of Zero Trust principles, strong engineering focus, and coordinated federal leadership.

European Union Approaches

The European Union has developed one of the most structured and regulation-driven approaches to Security-by-Design. Its cybersecurity model is shaped by strong emphasis on privacy, regulatory alignment, and cross-

border cooperation. A central pillar is the General Data Protection Regulation (GDPR), which requires Privacy-by-Design and Privacy-by-Default. In practice, this means systems must limit data collection to what is necessary and include built-in safeguards from the outset.

Organizations such as the European Union Agency for Cybersecurity (ENISA) provide technical guidance, architectural recommendations, and sector-specific security frameworks. These are often compared to U.S. standards but place greater emphasis on privacy, transparency, and accountability. In addition, widespread adoption of ISO/IEC 27001 strengthens risk management practices across both public and private sectors. Overall, the EU benefits from a highly coordinated governance structure that supports consistent implementation of SbD across member states.

Asia-Pacific Models

Countries in the Asia-Pacific region are increasingly integrating Security-by-Design into their digital and industrial systems. Nations such as Japan, South Korea, Singapore, and Australia are leading these efforts, particularly in areas like smart cities, industrial automation, and emerging technologies.

The approach often combines secure-by-default engineering with strong national cybersecurity strategies. For example, Singapore promotes SbD through strict certification programs and national digital trust initiatives, while Australia embeds security requirements into regulations for critical infrastructure sectors such as telecommunications, energy, and healthcare. Across the region, common priorities include innovation, national security, and technological sovereignty. As a result, SbD is increasingly viewed not just as compliance, but as a strategic necessity.

Africa and Latin America

In Africa and Latin America, the adoption of Security-by-Design is progressing more gradually, largely due to resource constraints, limited infrastructure, and skills shortages. However, there are clear signs of progress.

In Africa, countries such as Kenya, Nigeria, and South Africa are strengthening their cybersecurity frameworks. Nigeria's NDPR, for example, incorporates privacy principles similar to GDPR, while Kenya and South Africa continue to expand national cybersecurity strategies and regulatory structures.

In Latin America, countries like Brazil have made significant progress through laws such as the LGPD, which reflects GDPR-style data protection principles. Mexico and Chile are also developing stronger governance frameworks, although implementation varies across sectors. Despite ongoing challenges, both regions are steadily moving toward improved regulatory alignment and stronger cybersecurity practices.

Challenges Across Global Ecosystems

Despite growing interest in Security-by-Design (SbD),

its global adoption remains uneven and challenging. One major issue is the fragmentation of regulations across different regions, which creates inconsistencies and makes compliance more difficult for multinational organizations. In addition, supply chain vulnerabilities continue to pose serious risks, especially as organizations rely heavily on third-party vendors and increasingly complex cloud environments.

The rapid expansion of IoT devices has also widened the global attack surface. Many of these devices are low-cost and lack adequate security controls, making them easy targets for exploitation. At the same time, there is a global shortage of skilled cybersecurity professionals, which limits the ability of many countries, particularly developing ones—to fully implement SbD practices.

Geopolitical tensions and the rise of cyber warfare further complicate the situation by increasing the likelihood of targeted attacks and reducing the chances of global alignment on cybersecurity standards. Addressing these challenges will require stronger governance, better international cooperation, and more consistent security frameworks. Without coordinated efforts, gaps in implementation will continue to expose vulnerabilities across interconnected digital systems.

CONCLUSION

Security-by-Design (SbD) has become essential for securing modern digital infrastructures as technologies such as cloud computing, 5G, and IoT continue to expand. This study shows that while SbD is gaining global traction, its implementation varies across regions. The United States leads with strong federal mandates and widespread adoption of Zero Trust principles, while the European Union emphasizes regulatory frameworks centered on privacy and data protection. In contrast, Asia-Pacific countries are advancing SbD through innovation and national cybersecurity strategies, whereas Africa and Latin America are making gradual progress despite resource and capacity constraints.

Despite these differences, there is a shared recognition that SbD is critical for building resilient and trustworthy systems. However, challenges such as regulatory fragmentation, supply chain risks, and workforce shortages continue to limit its full adoption.

To address these gaps, this study recommends greater alignment of global security standards, stronger protection of software supply chains, broader adoption of Zero Trust models, increased investment in cybersecurity skills development, and improved international collaboration. Coordinated efforts in these areas will be key to ensuring consistent and effective implementation of Security-by-Design worldwide.

Closing Statement

Security is no longer just one aspect of future networks—it is becoming a fundamental requirement. Security-by-Design should move beyond being viewed as the best practice and instead be treated as a standard approach

across all digital systems. Achieving this will depend on strong governance, continued innovation, and closer international cooperation to ensure that the next generation of digital infrastructure is secure, reliable, and resilient.

REFERENCES

- Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, 53–66. <https://doi.org/10.1016/j.ijcip.2014.12.002>
- Adu-Gyimah, S., Kufour Boansi, O., Asante, G., & Addo, P. C. (2025). Academic trust betrayed: Unravelling the factors behind lecturers' vulnerability to social engineering attacks. *American Journal of Education and Technology*, 4(3), 53–61. <https://doi.org/10.54536/ajet.v4i3.4773>
- Alharkan, I., & Aslam, N. (2021). Zero trust in cloud computing: A systematic review. *IEEE Access*, 9, 160027–160047. <https://doi.org/10.1109/ACCESS.2021.3132025>
- Badr, Y., Chbeir, R., & Abraham, A. (2020). Security and resilience of next-generation cyber-physical systems. *Future Generation Computer Systems*, 108, 360–361. <https://doi.org/10.1016/j.future.2020.03.044>
- Cisco. (2023). *Zero-trust and secure-by-design networking: Architecture white paper*. <https://www.cisco.com>
- Cybersecurity and Infrastructure Security Agency. (2021). *Zero trust maturity model*. <https://www.cisa.gov>
- European Union Agency for Cybersecurity. (2021). *Access control and identity management guidelines*. <https://www.enisa.europa.eu>
- Fazil, A. W., Hakimi, M., Sajid, S., Quchi, M. M., & Khaliqyar, K. Q. (2023). Enhancing internet safety and cybersecurity awareness among secondary and high school students in Afghanistan: A case study of Badakhshan Province. *American Journal of Education and Technology*, 2(4), 50–61. <https://doi.org/10.54536/ajet.v2i4.2248>
- Forrester Research. (2010). *No more cheny centers: Introducing the Zero Trust model of information security* (J. Kindervag).
- Green, M., & Smith, M. (2016). Developers are not the enemy!: The need for usable security-by-design. *IEEE Security & Privacy*, 14(5), 40–46. <https://doi.org/10.1109/MSP.2016.88>
- Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Guide to attribute-based access control (ABAC): Definitions and considerations (NIST SP 800-162). *National Institute of Standards and Technology*. <https://doi.org/10.6028/NIST.SP.800-162>
- International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems—Requirements*.
- Kissel, R., Scholl, M., & Stine, K. (2012). Security considerations in the system development life cycle (NIST SP 800-64 Rev. 2). *National Institute of Standards and Technology*. <https://doi.org/10.6028/NIST.SP.800-64r2>
- Li, F., Hadjieleftheriou, M., Kollios, G., & Reyzin, L. (2005). Dynamic authenticated index structures for outsourced databases. *The VLDB Journal*, 14(4), 438–463. <https://doi.org/10.1007/s00778-005-0168-2>
- National Institute of Standards and Technology. (2013). *Security and privacy controls for federal information systems and organizations* (NIST SP 800-53 Rev. 4). <https://doi.org/10.6028/NIST.SP.800-53r4>
- National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST SP 800-207). <https://doi.org/10.6028/NIST.SP.800-207>
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266–2279. <https://doi.org/10.1016/j.comnet.2012.12.018>
- Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278–1308. <https://doi.org/10.1109/PROC.1975.9939>
- Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. W. W. Norton.
- Srinivas, J., Das, A. K., & Kumar, N. (2019). Secure access control techniques in cloud computing: A comprehensive survey. *Security and Communication Networks*, 2019, 1–30. <https://doi.org/10.1155/2019/8671864>
- Stallings, W. (2020). *Network security essentials: Applications and standards* (7th ed.). Pearson.
- Sullivan, C., & Burger, E. (2017). Cybersecurity: A human-centric approach. *American Journal of Law & Medicine*, 43(2–3), 365–381. <https://doi.org/10.1177/0098858817738222>
- UK National Cyber Security Centre. (2020). *Principles for Zero Trust architecture*. <https://www.ncsc.gov.uk>
- U.S. Executive Office of the President. (2021). *Executive Order 14028: Improving the nation's cybersecurity*. <https://www.whitehouse.gov>
- Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer. <https://doi.org/10.1007/978-3-319-57959-7>
- Zetter, K. (2015). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishing.