World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

The growing importance of cybersecurity in society: A quality engineering perspective

Jainik Sudhanshubhai Patel *

Cisco Systems, Inc., USA.

World Journal of Advanced Research and Reviews, 2025, 26(01), 4185-4192

Publication history: Received on 22 March 2025; revised on 27 April 2025; accepted on 30 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1457

Abstract

This article examines the evolving role of Quality Engineering (QE) in addressing modern cybersecurity challenges. It explores how traditional security testing approaches are being transformed through shift-left methodologies that integrate security throughout the software development lifecycle. The article analyzes key components of effective security-focused quality engineering, including automated testing frameworks, performance testing, secure code validation, and continuous monitoring. It examines regulatory compliance through an engineering lens, highlighting how automation and documentation contribute to both security and regulatory adherence. The article also presents organizational strategies for implementing security-first quality engineering, focusing on Develops integration, team expertise development, resource allocation, and ROI measurement. Finally, the article considers future directions, examining AI's impact on security testing and the role of quality engineering in building digital trust and societal resilience against cyber threats.

Keywords: Cybersecurity; Quality Engineering; Develops; Shift-Left Security; Digital Trust

1. Introduction

In today's hyperconnected world, cybersecurity has emerged as a cornerstone of digital society, evolving from a specialized IT concern into a fundamental societal imperative. The global cybersecurity market is projected to grow from $155.83 billion in 2022 to $376.32 billion by 2029, representing a compound annual growth rate of 13.4% during the forecast period [1]. This substantial growth reflects the increasing recognition of cybersecurity as an essential infrastructure rather than merely an optional business investment.

The sophistication of cyber threats has increased dramatically, with threat actors employing advanced persistent threats (APTs), zero-day exploits, and AI-powered attack vectors. The rising adoption of IoT, the surge in e-commerce platforms, and the proliferation of smart devices have dramatically expanded the attack surface for malicious actors [1]. These modern cyber threats are characterized by their persistence, stealth, and increasing ability to circumvent traditional security measures, necessitating more comprehensive defensive strategies.

At this critical juncture, Quality Engineering (QE) has emerged as a vital discipline in strengthening cybersecurity postures. As organizations increasingly deploy cloud computing solutions and engage in digital transformation initiatives, the integration of security practices within quality engineering frameworks has become essential for maintaining robust security postures while enabling innovation [1]. This convergence of disciplines represents a significant shift in how organizations approach digital security, moving beyond isolated security testing toward holistic quality-security integration.

* Corresponding author: Jainik Sudhanshubhai Patel

The transition from reactive to proactive security approaches marks perhaps the most significant paradigm shift in modern cybersecurity strategy. With cyber threats becoming more sophisticated and the cost of data breaches continuing to rise—averaging $4.24 million per incident according to recent industry reports—organizations are recognizing that post-breach responses are insufficient [1]. This shift-left approach embeds security considerations throughout the software development lifecycle rather than treating security as a final checkpoint, dramatically improving an organization's security posture while reducing remediation costs.

2. The Evolution of Security Testing in Quality Engineering

Traditional security testing models have demonstrated significant limitations in addressing the complex threat landscape of modern digital environments. According to comprehensive industry analysis, conventional security testing approaches detect vulnerabilities at a point when remediation costs are already at a premium, with the average cost to fix a bug found in the testing phase being substantially higher than one identified during the design phase [2]. This inadequacy stems primarily from siloed testing processes that occur too late in the development lifecycle, creating a problematic scenario where security becomes an afterthought rather than an integral component of the development process. Organizations continue to face extensive security debt, with a majority of codebases containing outdated components with at least one vulnerability, demonstrating how conventional approaches fail to address security comprehensively [2].

The emergence of "shift-left" security integration represents a paradigm shift in quality engineering approaches to cybersecurity. This methodology advocates for the integration of security testing throughout the software development lifecycle (SDLC), beginning with the earliest design phases. Organizations implementing shift-left security practices recognize that identifying and addressing security issues earlier in the development lifecycle reduces both the time and cost of remediation significantly. A proactive approach to security testing embedded within quality engineering practices can reduce the average time to remediate critical vulnerabilities substantially while simultaneously reducing overall security costs [2]. These improvements stem from addressing vulnerabilities when they are simpler and less expensive to fix.

The July 2024 CrowdStrike Falcon outage provides a compelling case study of how quality engineering deficiencies can create widespread security implications. The incident, triggered by a faulty update to CrowdStrike's Falcon sensor software, resulted in the crash of numerous Windows-operated computers globally, disrupting operations across healthcare, aviation, banking, and retail sectors. This event underscores the critical importance of comprehensive quality engineering practices that incorporate rigorous security testing before deployment, particularly for software that operates at a foundational level within critical systems.

Table 1 Security Testing Evolution in Quality Engineering [2, 3]

Key Aspect	Traditional Approach	Modern "Shift-Left" Approach
Timing of Security Testing	Late in development lifecycle	Throughout SDLC, beginning with design phases
Security Integration	Security as an afterthought	Security as an integral component
Cost Implications	Higher remediation costs	Reduced time and cost of remediation
Example Case Study	CrowdStrike Falcon outage (July 2024) - faulty update crashed 8.5 million Windows computers	Comprehensive quality engineering with rigorous security testing before deployment
Application to Critical Infrastructure	Systems face unique vulnerabilities due to distributed nature and legacy components	Specialized quality engineering approaches essential for protection

Modern critical infrastructure systems exhibit persistent vulnerabilities that represent significant national and economic security concerns. Critical infrastructure protection has become increasingly challenging as these systems face growing threats from both physical and cyber-attacks [3]. The interconnectedness of modern infrastructure systems—spanning energy, transportation, telecommunications, banking, and emergency services—creates complex interdependencies where failures can cascade across multiple sectors. Research indicates that a significant majority of critical infrastructure is owned and operated by the private sector, creating additional challenges in implementing consistent security standards [3]. These systems face unique vulnerabilities due to their distributed nature, increased

connectivity, and often legacy components that were not designed with modern security requirements in mind, demonstrating why specialized quality engineering approaches are essential for their protection.

3. Quality Engineering Methodologies for Enhanced Cybersecurity

Automated security testing frameworks have revolutionized how organizations identify and remediate software vulnerabilities throughout the development lifecycle. Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Interactive Application Security Testing (IAST) represent critical components of the Building Security In Maturity Model (BSIMM), which has documented security practices across numerous participating organizations [4]. The BSIMM framework identifies automated security testing as one of the core practices within its "Intelligence" domain, with many surveyed organizations implementing code review tools and integrating security tools into the development environment. Organizations implementing these tools in alignment with BSIMM guidelines demonstrate measurable improvements in vulnerability detection rates, with high-maturity organizations detecting significantly more security issues than low-maturity organizations. The BSIMM data further reveals that organizations with established Software Security Groups (SSGs) demonstrate a higher implementation rate of automated security testing tools compared to organizations in early security maturity stages [4].

Performance and resilience testing protocols constitute critical components of modern cybersecurity quality engineering. According to comprehensive research on cybersecurity metrics, resilience testing represents a fundamental approach to assessing an organization's ability to maintain essential functions during and after cyber incidents [5]. This research indicates that organizations should focus on measuring both the technical aspects of cyber resilience (such as time to detect, respond to, and recover from incidents) and the operational impacts (such as service availability and recovery capabilities). Performance testing under various attack scenarios allows organizations to establish baseline metrics for normal operations and identify their ability to withstand and recover from attacks. Proper measurement of these capabilities requires the establishment of quantifiable metrics that can be consistently tracked over time, such as mean time to recovery (MTTR) and percentage of service availability during attack scenarios [5].

Secure code and API validation techniques represent foundational practices in quality engineering for cybersecurity. The BSIMM framework identifies code review as one of the most widely adopted practices across surveyed organizations, implementing some form of security-focused code review [4]. API security validation is particularly emphasized within BSIMM's "Software Environment" domain, which focuses on configuration management and vulnerability management. The implementation of secure coding standards varies significantly across organizations, with BSIMM data indicating that high-maturity organizations are more likely to have established formal secure coding standards compared to low-maturity organizations. The model demonstrates a clear correlation between the implementation of secure coding practices and reduced vulnerability rates, with organizations at the highest maturity level experiencing fewer vulnerabilities per thousand lines of code compared to organizations at the lowest maturity level [4].

Continuous security monitoring implementation closes the cybersecurity quality engineering loop by providing real-time visibility into system behavior and potential threats. Research on cybersecurity metrics emphasizes that continuous monitoring represents a critical capability for effective detection and response to cyber incidents [5]. Effective cybersecurity metrics for monitoring include both leading indicators (which predict future performance) and lagging indicators (which measure past performance), creating a comprehensive view of security posture. Organizations should implement metrics that span across technical, operational, and strategic levels to ensure comprehensive visibility. The research specifically highlights the importance of establishing baseline performance metrics through continuous monitoring to accurately detect anomalies that may indicate security incidents. Furthermore, the study emphasizes that organizations must move beyond simply collecting monitoring data to establishing meaningful thresholds and taking action when those thresholds are exceeded [5].

Table 2 Quality Engineering Methodologies for Enhanced Cybersecurity [4, 5]

Methodology	Key Components	Benefits
Automated Security Testing Frameworks	SAST, DAST, and IAST within BSIMM framework	Improved vulnerability detection rates; higher implementation through Software Security Groups (SSGs)
Performance and Resilience Testing	Technical aspects (detection, response, recovery time) and operational impacts (availability, recovery capabilities)	Establishes baseline metrics; identifies ability to withstand and recover from attacks
Secure Code and API Validation	Security-focused code review; API security validation within "Software Environment" domain	Reduces vulnerability rates; correlation between secure coding practices and fewer vulnerabilities
Continuous Security Monitoring	Leading indicators (predict future performance) and lagging indicators (measure past performance)	Real-time visibility into system behavior and potential threats; enables anomaly detection
Implementation Maturity Levels	BSIMM maturity levels from low to high	High-maturity organizations experience better security outcomes across all methodologies

4. Regulatory Compliance Through Engineering Excellence

Key cybersecurity regulations have emerged as significant drivers for organizational security practices, imposing substantial requirements and potential penalties for non-compliance. The General Data Protection Regulation (GDPR) imposes significant fines for serious violations, representing a substantial financial risk for non-compliant organizations [6]. Organizations must carefully evaluate the economics of cybersecurity investments against these potential regulatory penalties, with research indicating that preventative security measures typically cost significantly less than the consequences of breaches or non-compliance. A comprehensive cybersecurity program requires investments in technology, personnel, training, and ongoing maintenance, with studies estimating that organizations allocate a portion of their IT budgets to security functions, though this varies substantially by industry and regulatory requirements [6]. The economic calculus of compliance requires balancing these direct investment costs against both tangible factors (such as regulatory penalties and breach remediation) and intangible factors (such as reputation damage and loss of customer trust).

Automated governance and compliance verification tools have revolutionized how organizations approach regulatory requirements, reducing manual effort while improving accuracy and coverage. Compliance automation tools streamline the process of collecting evidence, monitoring controls, and producing the documentation required for audits across frameworks like SOC 2, ISO 27001, HIPAA, and others [7]. Organizations implementing compliance automation report significant efficiency gains, with manual compliance processes typically requiring weeks of preparation for each audit, while automated systems can reduce this to days or even hours. These solutions provide real-time visibility into compliance status through centralized dashboards, allowing organizations to identify and address gaps proactively rather than reactively during audit periods. The most effective compliance automation tools integrate directly with cloud infrastructure, SaaS applications, and internal systems to continuously monitor security controls and provide evidence of their effectiveness without requiring manual intervention [7].

Documentation and traceability in security testing serve as critical components of regulatory compliance, providing evidence of due diligence and supporting audit activities. The economics of cybersecurity demonstrates that comprehensive documentation represents a significant factor in reducing both compliance costs and security risks [6]. Organizations must evaluate the return on investment for security documentation practices, considering both the direct costs of maintaining documentation and the potentially higher costs of inadequate documentation during security incidents or regulatory investigations. Research indicates that mature documentation practices contribute to more efficient incident response, with organizations able to identify and remediate threats significantly faster when proper security documentation exists. Furthermore, the cost-benefit analysis of security investments becomes more accurate when organizations maintain detailed records of security incidents, allowing for data-driven decisions about future security investments [6].

Building compliance into the development lifecycle represents the most effective approach to achieving sustainable regulatory adherence while minimizing friction with innovation objectives. Modern compliance automation platforms enable organizations to embed compliance requirements directly into development workflows through API-based integrations with development tools and infrastructure [7]. Organizations can implement continuous compliance monitoring that aligns with continuous integration/continuous deployment (CI/CD) pipelines, ensuring that compliance checks occur automatically alongside other quality verification steps. These automated systems can provide immediate feedback to development teams when potential compliance issues arise, allowing for rapid remediation before code reaches production environments. Furthermore, compliance automation tools can generate and maintain the necessary documentation that demonstrates adherence to regulatory requirements, creating an auditable trail of evidence that significantly reduces the manual effort typically associated with compliance activities [7].

Table 3 Regulatory Compliance Through Engineering Excellence [6, 7]

Key Aspect	Challenges	Engineering Solutions
Cybersecurity Regulations	Substantial requirements and penalties (e.g., GDPR fines); balancing investment costs against regulatory penalties	Preventative security measures; comprehensive investment in technology, personnel, training and maintenance
Compliance Verification	Manual processes requiring weeks of preparation; reactive approaches during audit periods	Automated governance tools; streamlined evidence collection across frameworks (SOC 2, ISO 27001, HIPAA)
Documentation and Traceability	High costs of inadequate documentation during incidents; difficulty evaluating ROI for security practices	Comprehensive documentation systems; detailed records of security incidents enabling data-driven decisions
Development Lifecycle Integration	Friction between compliance and innovation objectives; delayed remediation of compliance issues	Compliance requirements embedded in development workflows; API-based integrations with development tools
Continuous Monitoring	Manual intervention requirements; reactive compliance management	Real-time visibility through centralized dashboards; automated checks within CI/CD pipelines; immediate feedback to development teams

5. Organizational Strategies for Security-First Quality Engineering

Integrating DevSecOps across the enterprise represents a fundamental shift in how organizations approach security within their quality engineering practices. The DevSecOps Maturity Model defines distinct maturity levels that organizations typically progress through: Basic DevOps with minimal security integration, DevSecOps with initial security tooling, DevSecOps with deeper security integration, and ultimately Advanced DevSecOps with full security automation [8]. This evolution involves progressively embedding security across key capability areas: collaboration and culture, application security, infrastructure-as-code (IaC) security, identity and access management, continuous integration/delivery (CI/CD) pipeline security, compliance-as-code, monitoring, and threat modeling. Each capability area requires specific technical practices, with organizations typically starting with vulnerability scanning and gradually advancing to more sophisticated practices such as automated security gates within CI/CD pipelines, comprehensive security unit testing, and container security across the entire software development lifecycle [8].

Building security awareness and expertise among Quality Engineering teams delivers measurable improvements in security outcomes. Organizations should establish security champions within agile teams, who serve as the connection point between security specialists and developers, helping to disseminate security knowledge throughout the organization [9]. These champions receive specialized security training and subsequently drive the adoption of security best practices within their teams. Effective security awareness programs implement "shift-left" security approaches that incorporate security considerations from the earliest stages of development, including threat modeling during the planning phase and security stories in the product backlog. These practices help transform security from a separate concern into an integral component of the quality engineering process, enabling teams to identify and address security issues when they are least expensive to fix [9].

Resource allocation for proactive security testing plays a critical role in establishing effective security-first quality engineering practices. As organizations progress through the DevSecOps maturity model, they must strategically allocate resources across different aspects of security testing, from basic practices like static application security testing (SAST) to more advanced approaches like interactive application security testing (IAST) [9]. The model recommends implementing security testing in phases aligned with organizational maturity, starting with fundamental controls and gradually expanding to more comprehensive security coverage. This phased approach allows organizations to prioritize their investments based on risk, focusing first on critical applications and infrastructure while gradually expanding security testing coverage as capabilities mature. Resource allocation decisions should be guided by the principle of minimizing the cost of security defects by detecting them as early as possible in the development lifecycle [8].

Measuring security ROI through quality metrics enables organizations to quantify the business value of security investments and optimize their security-first quality engineering approaches. Effective security metrics for agile teams should focus on actionable data that drives continuous improvement while maintaining a balance between security and delivery objectives [9]. Teams should implement metrics that track both security activities (such as the percentage of user stories with security requirements and the percentage of code covered by security testing) and security outcomes (such as the number of vulnerabilities identified and remediated during development versus production). The most effective approach combines automated security metrics as part of the CI/CD pipeline with regular security-focused retrospectives that address qualitative aspects of security integration. These metrics should evolve as teams mature, with increasing emphasis on preventative measures rather than reactive remediation, as security practices become more embedded in the quality engineering workflow [9].

Table 4 Organizational Strategies for Security-First Quality Engineering [8, 9]

Strategy	Implementation Approach	Benefits
DevSecOps Integration	Progressive maturity model from Basic DevOps to Advanced DevSecOps with full security automation	Embedding security across capability areas (collaboration, application security, IaC, IAM, CI/CD security, compliance-as-code, monitoring, threat modeling)
Security Awareness Building	Establishing security champions within agile teams; specialized security training	Connection between security specialists and developers; dissemination of security knowledge throughout organization
Shift-Left Security Approaches	Security considerations from earliest development stages; threat modeling during planning; security stories in product backlog	Security transformed from separate concern to integral component; issues addressed when least expensive to fix
Resource Allocation for Security Testing	Strategic allocation across testing types (SAST to IAST); phased implementation aligned with organizational maturity	Prioritization based on risk; focus on critical applications first; gradual expansion of security coverage
Security ROI Measurement	Actionable metrics tracking both security activities and outcomes; automated metrics in CI/CD pipeline with security-focused retrospectives	Quantification of business value; balance between security and delivery objectives; evolution toward preventative measures

6. Future Directions: Quality Engineering as a Cybersecurity Cornerstone

6.1. AI-Driven Security Testing

AI and machine learning technologies are fundamentally transforming predictive security testing within quality engineering practices. Organizations can now detect emerging threats before they materialize, gaining a critical advantage in the cybersecurity landscape. According to Palo Alto Networks, AI has become essential in addressing the scale and complexity of modern cyber threats, with the global AI cybersecurity market projected to grow significantly by the end of the decade [10].

Modern machine learning algorithms excel at detecting patterns and anomalies beyond human analytical capabilities, providing early warning systems for potential threats and enabling automated real-time attack responses. These AI-

powered security systems analyze vast datasets from multiple sources, identifying connections and threat indicators that traditional systems would miss.

The integration of AI into security testing delivers multiple benefits, including more accurate vulnerability detection, enhanced threat intelligence capabilities, and automated response mechanisms that reduce incident response times substantially. However, this technological advancement creates new challenges as adversaries increasingly leverage these same AI technologies to develop more sophisticated attacks. This has created an ongoing technological arms race requiring continuous advancement in defensive capabilities [10].

6.2. Digital Trust Through Quality Excellence

Building digital trust through quality excellence has emerged as a crucial competitive differentiator in today's market. According to UTU, digital trust represents the confidence that users, customers, and partners have in an organization's ability to create secure digital experiences while protecting their data and privacy [11].

Research indicates that businesses with high digital trust ratings experience significantly higher customer retention rates than competitors with lower trust scores. This trust becomes particularly critical as businesses increasingly rely on data-driven insights and digital transactions, with a majority of consumers indicating they would take their business elsewhere if they don't trust a company is handling their data responsibly [11].

Organizations that build digital trust through quality engineering practices benefit from stronger customer relationships, enhanced brand reputation, increased customer loyalty, and greater market competitiveness. Conversely, companies that suffer trust-damaging security breaches face significant consequences, with many consumers indicating they would avoid doing business with a company that experienced a data breach in the recent past [11].

6.3. Recommendations for Organizational Cybersecurity Maturity

To achieve sustainable security outcomes, organizations must address both technical practices and organizational culture. Key recommendations include implementing a comprehensive AI strategy that addresses both defensive applications and potential adversarial use cases, developing in-house AI expertise through targeted hiring and training programs, and establishing cross-functional teams combining security, data science, and quality engineering capabilities. Organizations should also focus on implementing robust data management practices to support AI model training, regularly assessing AI security tools against emerging threat vectors, maintaining human oversight of AI-driven security decisions, and establishing clear governance frameworks for AI implementation that align with regulatory requirements and ethical principles. As AI technologies continue to evolve rapidly, maintaining organizational agility through regular capability reassessment and adaptation becomes increasingly critical to maintaining effective security postures [10].

6.4. Quality Engineering and Societal Digital Resilience

Quality Engineering has become essential to societal digital resilience, serving as the foundation for secure and reliable critical infrastructure. As digital interactions become the primary means of conducting business, establishing trust through quality-engineered security practices creates a compelling competitive advantage [11].

Organizations that prioritize security quality engineering demonstrate greater resilience against evolving threats while building stronger stakeholder relationships. The implementation of comprehensive quality engineering practices enables organizations to create secure-by-design systems that maintain integrity and availability even under attack conditions.

Beyond individual organizational benefits, these practices contribute to broader societal resilience by protecting critical infrastructure and essential services from disruption. As digital systems become increasingly embedded in every aspect of modern life—from healthcare and finance to transportation and utilities—the quality of security engineering directly impacts societal stability and functionality. Organizations that recognize this broader responsibility and invest accordingly not only protect their own interests but contribute to the collective digital resilience that underpins modern society [11].

7. Conclusion

Quality Engineering has evolved from a traditional testing function to become a cornerstone of effective cybersecurity strategy in our increasingly digital society. By embedding security considerations throughout the development lifecycle

rather than treating them as an afterthought, organizations can identify vulnerabilities earlier, reduce remediation costs, and build more resilient systems. The integration of security within quality practices—supported by automation, specialized expertise, appropriate resource allocation, and meaningful metrics—creates a foundation for both regulatory compliance and trust-building with stakeholders. As threats continue to evolve in sophistication, particularly with the advancement of AI technologies, the quality engineering discipline must likewise adapt to meet these challenges. Organizations that recognize quality engineering as essential to security posture not only protect their own interests but contribute to the collective digital resilience that underpins modern society. By making this investment in security-first quality engineering, organizations can better navigate complex threat landscapes while maintaining the innovation pace required in today's competitive environment.

References

[1] Fortune Business Insights, "Cyber Security Market Size, Share, Growth and Global Industry Analysis By Type & Application, Regional Insights and Forecast to 2024-2032," Market Research Report, 2024. https://www.marketresearch.com/Fortune-Business-Insights-Pvt-Ltd-v4286/Cyber-Security-Size-Share-Growth-37076898/

[2] Eddie Knight, "The Impact of Security Testing on an Organization," 2023. https://www.sonatype.com/blog/the-impact-of-security-testing-on-an-organization

[3] Cristina Alcaraz, and Sherali Zeadally, "Critical Infrastructure Protection: Requirements and Challenges for the 21st Century," 2015. https://www.researchgate.net/publication/272391570_Critical_infrastructure_protection_Requirements_and_challenges_for_the_21st_century

[4] Nicolas Montauban, "BSIMM (Building Security In Maturity Model): A Complete Guide," codific, 2025. https://codific.com/bsimm-building-security-in-maturity-model-a-complete-guide/

[5] DON SNYDER et al., "Measuring Cybersecurity and Cyber Resiliency," RAND Corporation, 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2703/RAND_RR2703.pdf

[6] SKILLOGIC, "The Economics of Cybersecurity: Cost-Benefit Analysis," 2024. https://skillogic.com/blog/the-economics-of-cybersecurity-cost-benefit-analysis/

[7] Anna Fitzgerald, "Why Compliance Automation is a Strategic Advantage for Modern Organizations," 2024. https://secureframe.com/blog/compliance-automation

[8] Check Point Software Technologies, "DevSecOps Maturity Model," 2025. https://www.checkpoint.com/cyber-hub/cloud-security/devsecops/devsecops-maturity-model/

[9] Chelsea Komlo, and Maria Gomez, "Incorporating Security Best Practices in Agile Teams," Thoughtworks 2016. https://www.thoughtworks.com/en-in/insights/blog/incorporating-security-best-practices-agile-teams

[10] Palo Alto Networks, "What are Predictions of Artificial Intelligence (AI) in Cybersecurity?" 2023. https://www.paloaltonetworks.com/cyberpedia/predictions-of-artificial-intelligence-ai-in-cybersecurity

[11] UTU, "Why Digital Trust is Essential to Scale Your Business Today," 2021. https://utu.io/blog/why-digital-trust-is-essential-to-scale-your-business-today/