Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| **RESEARCH ARTICLE**

Cybersecurity's Societal Impact: Protecting Critical Infrastructure through Integrated Security Operations

Vishnu Vardhan Reddy Singireddy
Independent Researcher, USA
Corresponding Author: Vishnu Vardhan Reddy Singireddy, **E-mail**: vishnusingireddy7476@gmail.com

| ABSTRACT

Digital evolution in today's society has transformed the cybersecurity landscape considerably. Cybersecurity has transitioned from the focused technical aspect it was erstwhile, to its current need as an essential protective role for contemporary civilization. This article investigates the increasing number of cybersecurity professionals required for safeguarding critical infrastructure allied to services such as healthcare, finance, energy, and transportation systems. The COVID-19 pandemic triggered this scenario by hastening the shift to remote work and revealing weaknesses present earlier in security systems, making the need for cohesive security operations evident. Through the investigation of ServiceNow ITSM integration, organizations demonstrate significant improvements in incident response abilities by creating unified platforms that streamline threat identification and resolution procedures. The worldwide implementation of CIS Benchmarks signifies a transformative change toward uniform security practices, offering consensus-driven recommendations that go beyond local regulations and facilitate uniform protection across various organizational settings. Current threat intelligence efforts monitoring nation-state actors and threat factions worldwide highlight the complex characteristics of today's cyber threats, requiring proactive defense measures that utilize frameworks such as MITRE ATT&CK to connect theoretical security ideas with real-world applications. This change signifies a wider societal acknowledgment that cybersecurity experts act as protectors of digital infrastructure, combining technical skills with awareness of far-reaching societal effects to uphold economic stability and public safety in a connected world.

| KEYWORDS

Cybersecurity Infrastructure Protection, Integrated Security Operations, Remote Work Security Architecture, Global Security Standards Framework, Proactive Threat Intelligence.

| ARTICLE INFORMATION

ACCEPTED:12 July 2025 **PUBLISHED:** 25 August 2025 **DOI:** 10.32996/jcsts.2025.7.8.126x

1. Introduction

The societal digital transformation has raised cybersecurity from a specialized technical field to a key foundation of contemporary civilization. With organizations relying more on interconnected systems for vital operations, the responsibilities of cybersecurity professionals have grown beyond conventional IT limits to include safeguarding essential services that billions rely on every day. The World Economic Forum's Global Risks Report 2025 emphasizes technological risks, including cybersecurity failures, as interconnected threats that worsen other worldwide risks, identifying cyberattacks as the fifth most critical risk in the next two years [1].

The report highlights that cyber insecurity has emerged as a major catalyst of global instability, with conflicts between states and geoeconomic rivalries triggering ripple effects due to digital infrastructure weaknesses. This change demonstrates a wider understanding that cyber threats endanger not just individual entities but also the very structure of society.

The COVID-19 pandemic hastened this change, compelling swift implementation of remote work systems and revealing weaknesses in conventional security frameworks. Research conducted by Nicholas Bloom and team at the National Bureau of Economic Research indicates that hybrid work models have emerged as the primary organizational structure, with employees spending an average of 1.4 days a week remote working in 2023, marking a five-fold rise from the pre-pandemic average of 0.25 days per week [2]. The research shows that 29 percent of workdays are now conducted from home, significantly changing the security boundaries that companies must protect. This change emphasized the need for cohesive security operations that can adjust to changing threat environments while preserving operational effectiveness. The research indicates that hybrid work arrangements persist due to productivity gains averaging 3-4 percent, despite the increased cybersecurity threats they pose. Modern cybersecurity experts need to combat complex issues that involve technical, organizational, and social dimensions. This requires an all-encompassing approach to protect infrastructure.

The increase in the attack surface has been especially evident in vital infrastructure sectors, where the merging of information technology and operational technology has resulted in new weaknesses. The Global Risks Report 2025 indicates that technological risks are becoming more intertwined with environmental and social issues, resulting in complex threats that conventional security methods struggle to manage effectively [1]. The survey within the report indicates that 33 percent of global leaders view cyberattacks on essential infrastructure as a major threat in the next ten years, highlighting an increasing recognition of the susceptibility of digital systems to both criminal and government-backed threats.

This article analyzes the societal effects of cybersecurity by focusing on integrated security operations, investigating how resources like ServiceNow ITSM, benchmarks like CIS, and proactive threat intelligence enhance a holistic defense approach. Examining these elements illustrates the evolution of the cybersecurity field and addresses the need to safeguard vital infrastructure in a time when digital and physical security are interconnected. The shift from office-based to distributed work settings has fundamentally changed security needs, requiring innovative strategies to safeguard the broader digital boundary that now includes millions of home offices globally.

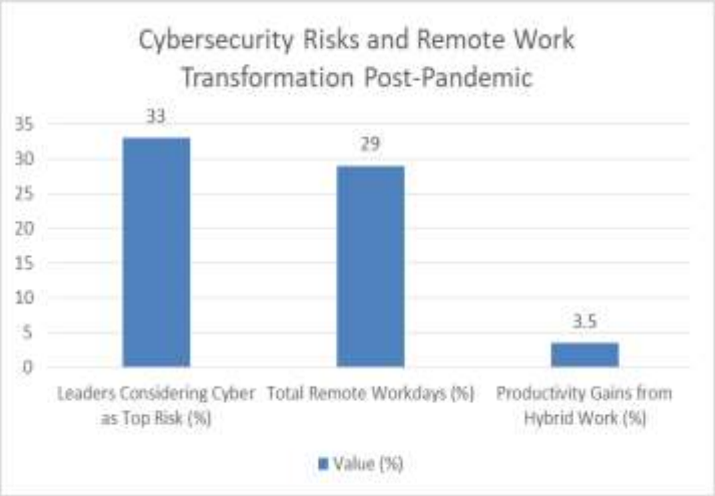

Figure 1: Cybersecurity Risks and Remote Work Transformation Post-Pandemic [1,2]

2. The Evolution of Cybersecurity as a Societal Imperative

The evolution of cybersecurity from a technical specialty to a societal essential signifies one of the most notable changes in contemporary professional environments. Originally limited to the protection of computer systems and networks, cybersecurity has evolved to include the defense of essential services such as healthcare systems, financial infrastructure, energy grids, and transportation networks. Studies conducted by Fabio De Felice and team offer an in-depth examination of the development of critical infrastructure, illustrating how these systems have progressively become more interconnected and digitalized in recent years [3]. The research highlights that critical infrastructures are "complex systems of systems," where a disturbance in one area can ripple through interconnected networks, impacting various vital services at once. This progress demonstrates the remarkable digital transformation of essential infrastructure and the resulting increase in the attack surface accessible to malicious entities.

The pandemic triggered this change by revealing weaknesses that had been present earlier and suddenly got highlighted by the swift transition to remote work. Organizations that previously depended on physical barriers and limited access for security now face the challenge of safeguarding remote employees accessing sensitive systems from various locations.

Chris Brown's examination of data breach expenses reveals that the average overall expense of a data breach has escalated considerably, as organizations experience both short-term financial losses and enduring damage to their reputation along with operational interruptions [4]. The study shows that breach expenses go well beyond initial recovery actions, including legal costs, regulatory penalties, customer alert costs, and operational disruption effects that can last for years following an event. This change in perspective heightened existing security concerns and brought forth new ones, forcing security professionals to adapt their approaches and assets quickly.

The advancement of critical infrastructure protection has evolved through distinct phases, as described by De Felice et al., moving from protecting standalone systems to securing integrated networks [3]. The researchers highlight three main evolutionary phases in this regard. The first is the pre-digital era, which prioritizes physical security. The second is the digital transformation stage, which concentrates on IT security. The third is the present convergence era, wherein cyber-physical systems necessitate comprehensive protection approaches. This transformation has greatly altered the duties of cybersecurity professionals, who must now understand complex links between digital and physical systems while protecting against threats that might arise from anywhere in the world.

The impact of cybersecurity failures on society has become more evident due to prominent events involving essential infrastructure. Ransomware strikes on healthcare facilities have interrupted patient services, cyber assaults on energy systems have endangered power availability, and compromises of financial networks have jeopardized economic security. Brown's study emphasizes that aside from short-term financial effects, data breaches lead to a drop in customer trust, causing organizations to face average churn rates that greatly affect long-term revenue [4]. The study shows that costs from breaches differ significantly by industry, with heavily regulated sectors and those managing sensitive personal information experiencing much higher remediation costs. These events show that cybersecurity has evolved beyond an IT issue and is now essential for ensuring public safety and the functioning of society. Security experts have therefore transformed from technical specialists to protectors of the digital framework on which contemporary society relies.

3. Integrated Security Operations Through ServiceNow ITSM

The combination of ServiceNow IT Service Management (ITSM) with monitoring tools signifies an important improvement in an organization's ability to respond to incidents. This integration establishes a cohesive platform that enhances the detection, analysis, and resolution of security incidents, greatly minimizing the duration between threat identification and its solution. Research by Maja Djurica et al. shows that initiatives for digital transformation, especially those that utilize integrated service management platforms, fundamentally alter business processes and improve user experiences throughout organizations [5].

The study reveals that successful digital transformation requires not merely technological implementation but comprehensive process reengineering that aligns IT operations with business objectives. By consolidating security operations within a comprehensive ITSM framework, organizations can achieve greater visibility into their security posture while improving coordination between security teams and other IT functions.

ServiceNow ITSM integration enables automated workflows that accelerate incident response processes. While detecting potential security threats, monitoring tools can automatically create incidents within ServiceNow, triggering predefined response procedures and notifying appropriate personnel. According to Sarah Wood's comprehensive analysis in the Security Operations Resource Library, organizations implementing integrated security operations platforms experience significant improvements in their security posture through enhanced visibility, automated response capabilities, and improved collaboration between teams [6]. Wood emphasizes that the key to successful security operations lies in breaking down silos between IT and security teams, enabling seamless information sharing and coordinated response efforts. This automation eliminates manual handoffs and reduces the risk of human error during critical response periods. The platform's capability to sustain detailed audit trails allows organizations to show adherence to regulatory standards and carry out extensive post-incident evaluations.

The ServiceNow ITSM integration facilitates a digital transformation that goes beyond just technology improvement to include essential shifts in how organizations manage security operations. Djurica et al. emphasize that effective digital transformation efforts need to address both technological abilities and human aspects, making sure that new systems improve rather than hinder user workflows [5]. Research shows that organizations that successfully carry out digital transformation realize improved operational effectiveness, superior decision-making abilities, and greater synchronization of IT services with business requirements. This all-encompassing method of transformation is especially vital in security operations, where response speed and precision can be the deciding factors between a minor incident and a significant breach.

The effect of this integration goes beyond technical efficiency to include greater organizational resilience. By reducing the time needed to identify and react to security breaches, organizations can greatly diminish the possible harm from cyberattacks. The resource library documentation created by Wood emphasizes that modern security operations require a platform approach that combines threat intelligence, vulnerability management, and incident response into a cohesive system [6]. A unified strategy such as this allows security teams to transition from reactive to proactive approaches, which facilitates easier detection and resolution of vulnerabilities and prevents their exploitation by threat actors.

This ability is very crucial for organizations offering necessary services, since prolonged interruptions can result in far-reaching effects on society. The integration of ServiceNow ITSM with security monitoring systems represents not only technological progress but also a strategic dedication to societal stability.

Transformation Aspect	Key Outcome
Process Reengineering	IT-business alignment
Automated Workflows	Reduced manual handoffs
Team Collaboration	Breaking down IT-security silos
Operational Efficiency	Enhanced decision-making
Documentation Practices	Improved audit trails
Security Posture	Proactive vulnerability management
Response Capability	Seamless information sharing

Table 1: ServiceNow Integration Benefits and Transformation Requirements [5,6]

4. Global Standards and the CIS Benchmarks Framework

The Center for Internet Security (CIS) Benchmarks have become the leading worldwide benchmark for cybersecurity best practices, offering organizations practical advice for protecting their digital environments. In contrast to regional rules or proprietary norms, CIS Benchmarks are created through a consensus-driven method that collects perspectives from governments, businesses, academic organizations, and worldwide security experts.

Research by Tahereh Hasani and team emphasizes the crucial link between implementing cybersecurity measures and organizational success, demonstrating that entities employing standardized security frameworks realize notable improvements in their security posture and operational effectiveness [7]. The research highlights that adopting cybersecurity goes beyond being a technical issue; it is a strategic necessity that significantly affects organizational resilience and competitive edge. This joint effort guarantees that the standards incorporate diverse viewpoints and tackle the entire range of security issues encountered by contemporary businesses.

The global recognition and validation of CIS Benchmarks stem from their practical relevance across diverse industries, regulatory environments, and organizational contexts. These benchmarks enable organizations to implement consistent security protocols across diverse geographic regions or industries by providing clear, technically detailed instructions for protecting various platforms and technologies. Venkat Marella's in-depth analysis of security configuration challenges in containerized environments highlights the crucial importance of standardized security metrics in addressing the intricacies of modern IT infrastructure [8]. Marella highlights that containerized environments present particular security challenges due to their dynamic nature, short durations, and complex interdependencies, requiring uniform configuration standards to maintain security at scale. This standardization is particularly vital for international corporations and those overseeing critical infrastructure that spans multiple jurisdictions.

The implementation of CIS Benchmarks represents a major shift in how organizations manage security configurations. Hasani et al. show that organizations employing comprehensive cybersecurity frameworks achieve improved operational efficiency in multiple domains, including reduced security incidents, greater compliance with regulations, and enhanced trust among stakeholders [7]. The research shows that embracing cybersecurity serves as a driver for overall organizational improvements, fostering process uniformity, enhancing documentation methods, and nurturing a culture of security consciousness throughout the organization. These benefits extend beyond simple security improvements to encompass operational efficiencies that positively impact overall organizational effectiveness.

The consensus-driven framework that supports the creation of CIS Benchmarks guarantees wider relevance than local regulations or private security standards. Individuals from diverse backgrounds offer distinct viewpoints on threat environments, regulatory obligations, and operational limitations, leading to suggestions that harmonize security efficiency with practical implementation. Marella's analysis of containerized environment security highlights the significance of community-developed standards, emphasizing that the swift advancement of container technologies demands security guidance that can swiftly adjust to new threats and technological developments [8]. The study highlights that effective security setup in contemporary settings necessitates both technical measures and organizational procedures to guarantee the regular implementation and upkeep of security protocols. This inclusive strategy has positioned CIS Benchmarks as a common language for cybersecurity, fostering cooperation among organizations and allowing for more efficient joint defense tactics against changing threats.

Implementation Area	Impact/Challenge
Security Incidents	Reduced occurrence
Regulatory Compliance	Enhanced adherence
Stakeholder Confidence	Improved trust
Container Dynamic Nature	Security complexity
Ephemeral Lifecycles	Configuration challenges
Process Standardization	Enterprise-wide improvements
Security Culture	Organizational awareness
Community-driven Standards	Agile security guidance

Table 2: CIS Benchmarks Adoption and Containerized Environment Challenges [7,8]

5. Threat Intelligence and Proactive Defense Strategies

The complexity and scale of contemporary cyber threats require equally advanced defense strategies. Current threat intelligence efforts monitor over 40 active nation-state actors and over 140 threat groups from 20 countries, highlighting the worldwide scope of the cybersecurity issue. Research by Kristel M. de Nobrega and colleagues emphasizes the crucial need to synchronize cybersecurity practices with theoretical frameworks, arguing that an integrated approach encompassing technical, organizational, and strategic elements is essential for effective cyber defense [9]. Research suggests that conventional security frameworks frequently neglect the intricacies of contemporary threat environments, where opponents use advanced strategies that take advantage of the discrepancies between theoretical security concepts and their actual execution.

A complicated threat environment urges security experts to adopt proactive defense methods rather than traditional reactive approaches, which in turn, enables them to foresee and avert attacks prior to their affecting essential systems.

Proactive prevention of threats depends on substantial intelligence collection and analytical abilities that allow organizations to recognize emerging threats and adjust their defenses accordingly. By examining the actions, strategies, methods, and processes (TTPs) of threat actors, security teams can uncover trends and signs that imply possible attacks.

Yuning Jiang and colleagues provide a thorough analysis of how the MITRE ATT&CK framework is applied in cybersecurity, demonstrating the impact this standardized approach to threat modeling has had on defensive strategies [10].

The researchers emphasize that the ATT&CK framework is crucial for connecting threat intelligence to actionable security measures, allowing organizations to associate adversary actions with particular defensive approaches. This intelligence-based strategy enables organizations to establish focused protections against particular threats instead of depending exclusively on traditional security methods.

The shift toward proactive defense strategies signifies a critical change in cybersecurity philosophy. De Nobrega et al. contend that successful cyber defense necessitates a shift from conventional perimeter-centric security models to adopt adaptive, intelligence-led strategies capable of addressing evolving threat environments [9]. The study highlights that contemporary cyber defense should include ongoing learning processes, allowing organizations to adjust their approaches according to new threats and changing enemy tactics. This flexible strategy is very essential considering the asymmetric character of cyber warfare, where attackers only need to succeed a single time, whilst defenders must remain alert every minute.

Community-oriented defense approaches have become an essential element of successful cybersecurity, acknowledging that no individual organization can tackle the entire range of threats on its own. Information-sharing initiatives allow organizations to capitalize on collective intelligence, gaining insights from incidents faced by peers and taking preventive steps before comparable attacks aim at their systems. Jiang et al. illustrate how the MITRE ATT&CK framework supports this cooperative method by offering a unified terminology for articulating adversary actions, which allows organizations to exchange threat intelligence more efficiently [10]. The research shows that companies engaged in threat intelligence sharing groups achieve higher detection rates and shorter dwell times for advanced persistent threats. This cooperative method illustrates the field's shift from separate technical groups to integrated communities collaborating to safeguard societal infrastructure, with the ATT&CK framework acting as a vital facilitator of this change.

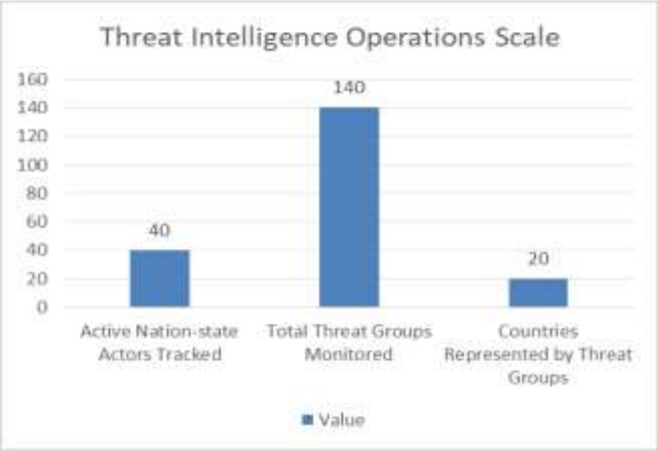

Figure 2: Threat Intelligence Operations Scale [9,10]

6. Conclusion

The evolution of cybersecurity from a specialized field to an essential societal requirement marks a sea change in how modern society protects its digital systems, which are comprised of multiple elements. The integration of sophisticated systems such as ServiceNow ITSM is one such change that has enabled automated incident management and the global adoption of uniform frameworks like CIS Benchmarks. The field has evolved to manage a broadened attack surface resulting from remote work settings and interconnected essential infrastructure, necessitating professionals to cultivate knowledge that covers technical, organizational, and social areas. The transition towards proactive defense tactics, in tandem with extensive threat intelligence and collaborative models such as MITRE ATT&CK, illustrates that the field has evolved from the erstwhile reactive technical teams to proactive protectors of critical services in contemporary times. With cyber threats growing in complexity and size, the cybersecurity field is required to advance towards unified, intelligence-led, and community-oriented defensive tactics. The future stability of a digital society looks towards cybersecurity experts who can merge technical proficiency with strategic insight. Such experts can ensure that essential infrastructure stays robust against a growing range of threats whilst allowing the advantages of digital transformation to extend to all sections of society.

Funding: This research received no external funding

Conflicts of interest: The authors declare no conflict of interest

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

References

[1] Chris B, (2025). The Real Cost of a Data Breach in 2025, Viking Cloud, Mar. 2025. [Online]. Available: https://www.vikingcloud.com/blog/the-real-cost-of-data-breach

[2] Fabio D F et al. (2022). Critical Infrastructures Overview: Past, Present and Future, ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/358664350_Critical_Infrastructures_Overview_Past_Present_and_Future

[3] Kristel M. N et al. (2024). The whole of cyber defense: Syncing practice and theory, ScienceDirect, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S096386872400043X

[4] Maja D et al. (2023). The Impact of Digital Transformation on Business Processes and User Experience, ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/377782667_The_Impact_of_Digital_Transformation_on_Business_Processes_and_User_Experience

[5] Nicholas B et al. (2023). How Hybrid Working From Home Works Out, National Bureau Of Economic Research, 2023. [Online]. Available: https://www.nber.org/system/files/working_papers/w30292/w30292.pdf

[6] Sarah W, (2024). Security Operations Resource Library, ServiceNow, 2024. [Online]. Available: https://www.servicenow.com/community/secops-articles/security-operations-resource-library/ta-p/3120885

[7] Tahereh H et al. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance, Springer Nature, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s43546-023-00477-6

[8] Venkat M, (2024). Challenges and Best Practices in Security Configuration for Containerized Environments, IJSRSET, 2024. [Online]. Available: https://ijsrset.com/index.php/home/article/view/IJSRSET24105471/IJSRSET24105471

[9] World Economic Forum, (2025). The Global Risks Report 2025 - 20th Edition, Jan. 2025. [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

[10] Yuning J et al. (2025). MITRE ATT&CK Applications in Cybersecurity and The Way Forward, arXiv, Feb. 2025. [Online]. Available: https://arxiv.org/html/2502.10825v1