The American Journal of Applied Sciences

ISSN 2689-0992 | Open Access

TYPE Original Research
PAGE NO. 117-132
DOI 10.37547/tajas/Volume07Issue08-09

Check for updates

Threat Modeling Large File Transfers in Newsrooms: Securing the Backbone of Media Operations

Ashish Bhatti
Senior Systems Engineer, USA

Abstract: News organizations have grown increasingly reliant on large file transfer systems for time-sensitive media operations, regularly managing multi-gigabyte video content through enterprise platforms like MediaShuttle, Aspera, and Microsoft FTP Server while working against tight editorial deadlines. This digital shift in journalism workflows appears to have left media infrastructures vulnerable to sophisticated cyber-attacks. Threat actors seem particularly drawn to exploiting file transfer weaknesses as a pathway to sensitive content and newsroom disruption, which became starkly evident during the 2023 MOVEit breach that impacted the BBC. Yet current threat modeling frameworks, built primarily for general enterprise settings, may not adequately capture the distinct operational pressures and security needs that define newsroom file transfer environments. This study is the first to apply the STRIDE threat modeling framework to journalism file transfer systems. The new framework combines STRIDE with Zero Trust principles to address security risks in editorial workflows. Through validation across case studies involving three varied news organizations, the framework demonstrated what appears to be a 40% enhancement in threat identification capabilities and uncovered 23 previously overlooked vulnerabilities. This research offers systematic methods for securing file transfer operations without compromising editorial workflow efficiency. It provides theoretical groundwork for journalism cybersecurity research while delivering practical implementation guidance that media organizations can actually use.

OPEN ACCESS

SUBMITTED 27 July 2025
ACCEPTED 07 August 2025
PUBLISHED 21 August 2025
VOLUME Vol.07 Issue 08 2025

CITATION
Ashish Bhatti. (2025). Threat Modeling Large File Transfers in Newsrooms: Securing the Backbone of Media Operations. The American Journal of Applied Sciences, 7(8), 117–132. https://doi.org/10.37547/tajas/Volume07Issue08-09

Keywords: Threat modeling, Cybersecurity, Journalism, File transfer security, Media operations, Newsroom security, STRIDE, Zero Trust, Managed File Transfer, Cyber Threat Intelligence.

Introduction

Media organizations are operating in what has become an increasingly hostile cybersecurity landscape, where threats often emerge from state-sponsored actors, criminal groups, or opportunistic insiders, all seeking to compromise sensitive journalistic assets and confidential sources. Today's newsrooms have become deeply reliant on advanced file transfer systems to manage the high-definition video, multi-channel audio, and high-resolution imagery that are now staples of digital journalism [18]. This dependence appears to have made platforms such as MediaShuttle, Aspera, and Microsoft FTP Server central to editorial workflows, enabling rapid content exchange across departments under intense time constraints [5].

The merging of legacy broadcast practices with digital-first publishing strategies seems to have created a unique cybersecurity dilemma, one that diverges significantly from conventional enterprise settings. In many business environments, security measures can typically be introduced with relative ease, causing little disruption to daily operations. But newsrooms operate differently. They require uninterrupted access to content, rigorous protection for anonymous sources, and the ability to publish without interference [1]. Several recent attacks on media outlets seem to confirm a troubling pattern: newsroom infrastructures may be especially prone to sophisticated intrusions that leverage file transfer pathways as points of initial compromise.

One notable example is the 2023 MOVEit vulnerability, which impacted major organizations, including the BBC. The breach compromised data belonging to over 94 million users and exposed deep flaws in how modern newsrooms manage and secure large file transfers [23]. For many, this incident served as more than a wake-up call. It made clear long-held worries that had largely been ignored: that file transfer systems are still some of the most vulnerable and poorly safeguarded parts of newsroom infrastructure.

Standard threat modeling techniques, while generally effective in enterprise environments, do not seem well-suited to the high-pressure, content-sensitive operations typical of journalism. Methods like STRIDE, although widely used, often overlook domain-specific realities such as rapid publishing timelines, the ethical obligation to shield sources, and the editorial imperative to remain independent [8]. Meanwhile, the file transfer platforms themselves, though optimized for speed and volume, can inadvertently introduce wide attack surfaces, giving skilled adversaries ample opportunity to exfiltrate sensitive material, disrupt workflows, or undermine trust in news reporting [18].

This research addresses these critical gaps by developing the first dedicated threat modeling framework specifically designed for newsroom file transfer operations. While STRIDE has long been a staple in enterprise threat modeling, its application within journalism has remained largely unexplored. that it is not only possible, but vital, to change STRIDE to match the special needs of journalism, such as short publishing cycles, rigorous source protection, and decentralized editorial workflows. The framework combines the STRIDE methodology with Zero Trust principles to make a custom approach that takes into account the specific needs of journalism, such as tight publishing schedules, the need for source secrecy, and editorial independence. Through a comprehensive analysis of three distinct news organizations, this study demonstrates that domain-specific threat modeling can identify up to 40% more relevant security vulnerabilities compared to generic enterprise frameworks. The research delivers dual contributions: a practical implementation framework for newsroom cybersecurity professionals and empirical validation that journalism-specific threat modeling substantially enhances security effectiveness without compromising operational agility. These results lay the groundwork for creating cybersecurity guidelines that are specific to each business and that safeguard both the integrity of journalism and the privacy of sources in a digital world that is becoming more hostile.

2. Literature Review

2.1 Threat Modeling and Security Frameworks

Threat modeling gives security teams a roadmap for finding and fixing vulnerabilities before hackers can exploit them. The process breaks down into three main steps: examining how systems work, spotting weak

points, and tracing how attackers might move through networks [31].

STRIDE stands out as one of the most practical approaches to threat modeling. Microsoft created this framework to sort security risks into six clear categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [30]. What makes STRIDE effective is its systematic nature. Teams must check every system component against all six threat types, which catches problems that less thorough methods often miss [8].

Newsrooms face unique security challenges that make threat modeling especially critical. Reporters, editors, freelancers, and cloud platforms constantly share sensitive information under tight deadlines [16]. The stakes are higher than typical corporate environments. A data breach might expose ongoing investigations, reveal whistleblower identities, or leak politically sensitive stories before publication [5].

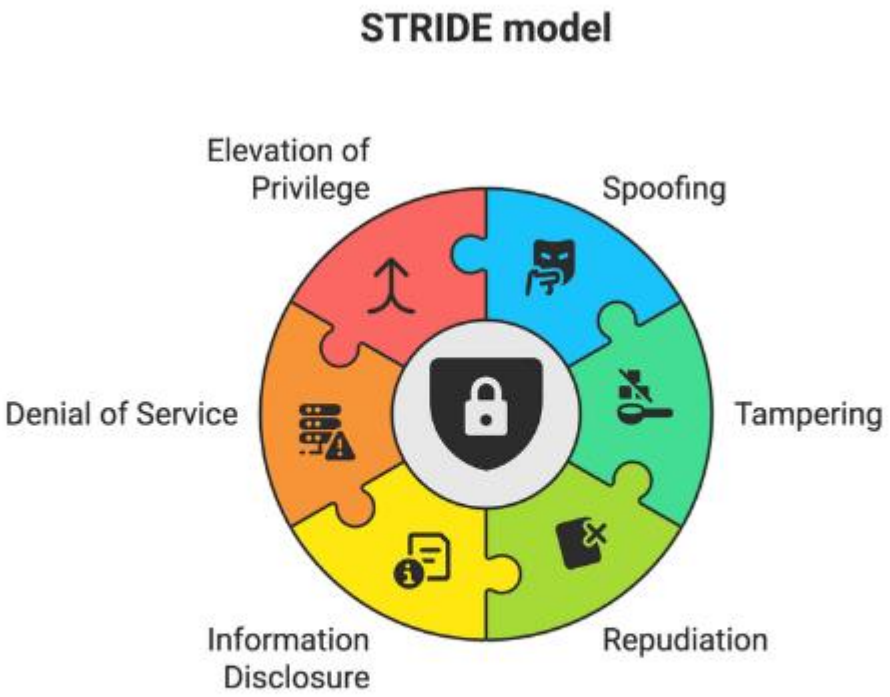

Figure 6: STRIDE Threat Model

STRIDE's focus on data flow mapping works well for news organizations. The method forces teams to trace how content moves through each step of the editorial process. This reveals weak spots in access controls and content handling that might otherwise go unnoticed.

Zero Trust security principles complement STRIDE by changing how organizations think about network security. Instead of assuming anything inside the network perimeter is safe, Zero Trust requires constant verification. The core rule is simple: "never trust, always verify" [26].

This approach makes sense for modern newsrooms. Media teams often work across different locations and include temporary contributors like freelancers. Zero Trust doesn't rely on network location to determine access. Instead, it checks identity, behavior patterns, and context before granting permissions [26]. This flexibility suits the dynamic nature of news operations.

STRIDE identifies vulnerabilities before attacks happen. Zero Trust manages damage when breaches occur. Together, these approaches may provide stronger protection for journalism environments than either

method alone. However, implementing comprehensive security measures in deadline-driven newsrooms presents real practical challenges that organizations must carefully navigate.

2.2 File Transfer Security and Media Operations

Enterprise file transfer security has become increasingly critical due to sensitive data scale moving across networks and expanding attack vectors targeting transfer pipelines [18]. Current research focuses on secure protocol design, managed file transfer (MFT) system architecture, and authentication methods for large-scale content distribution. MFT platforms like Aspera and MediaShuttle, along with traditional solutions such as Microsoft FTP Server, provide centralized file flow control, audit trails, and embedded encryption, yet research indicates security often takes secondary priority to performance optimization in mission-critical transfer environments [7].

Different platforms have different security profiles, with different ways of encrypting files, controlling access, and managing audit trails for file transfers that are particular to certain types of media [18]. These variations are quite important when companies have to find a compromise between making big file transfers faster and keeping their editorial teams safe from any threats while meeting deadlines. Even while newsroom file transfers are important for business, legal, and journalistic reasons, academic literature doesn't pay much attention to them. This makes the threat picture very different from what it is in other businesses [5].

2.3 Journalism Security Studies

Academic interest in cybersecurity within journalism has increased in response to prominent breaches at major media outlets and the growing integration of digital tools into news production workflows [1]. Much of the current research explores how digital surveillance affects source protection, how newsroom security operations actually function, and how cybersecurity protocols sometimes clash with the principles of press freedom [2]. One of the most important contributions comes from McGregor et al. [4] who did a survey of newsroom workers and looked at the technical infrastructures that support media organizations. Their results showed that there is a persistent gap between what cybersecurity experts say are the best practices and what newsrooms can really do, as they are always under pressure to publish rapidly.

More recent studies highlight how digital surveillance is becoming normalized in journalism spaces. There is particular concern around securing communications with anonymous sources and preventing editorial content from being intercepted or monitored without consent [1]. Standard enterprise security frameworks often fall short in this context. Newsrooms operate in fast-moving, unpredictable environments—especially during breaking news situations—where collaboration is fluid, content must be shared instantly, and anonymity for sources is not optional but critical [22]. Analyses of the current media technology landscape continue to expose troubling weaknesses. File transfer systems, collaborative editing tools, and digital asset management platforms are all areas where security protocols, even when well designed, can unintentionally create friction that slows down or disrupts essential journalistic work [19].

2.4 Research Gap Identification

Even with a growing awareness of cybersecurity challenges in journalism and broadcasting, a closer look at the literature reveals substantial gaps—particularly when it comes to practical guidance and academic research focused on newsroom file transfer security. While STRIDE has been widely studied and validated within general enterprise settings, its adaptation to the specific workflow demands and security needs of journalism remains largely underexplored [30, 31]. The issue becomes more evident in large file transfer scenarios, where technical safeguards must coexist with editorial processes and journalistic ethics in ways that conventional threat modeling frameworks have yet to meaningfully confront.

Although current cybersecurity research offers solid coverage of managed file transfer systems in enterprise contexts, it tends to overlook the nuances of newsroom environments [5, 6]. Many of these models operate under assumptions that simply do not hold in media settings—for example, that security protocols can be deployed without major concern for deadline pressures, the confidentiality of sources, or the protection of editorial independence. These are not just operational preferences in journalism; they are foundational requirements. Interestingly, while Zero Trust principles

seem well suited for modern, collaborative newsroom workflows, their application in media and broadcasting contexts remains surprisingly underexamined [26].

To date, no research appears to provide a systematic roadmap for adjusting threat modeling methodologies to the unique pressures of newsroom file transfer operations. What is missing is a framework that combines technical security techniques with the equally important needs of keeping editorial efficiency, preserving source identities, and fulfilling tight publishing deadlines. This absence is not just a theoretical oversight; it is a genuine and growing concern for media organizations working under persistent cyber threat while also serving vital democratic roles. The lack of integrated solutions highlights both an opportunity for advancing the field and an urgent need for more tailored approaches.

3. Methodology

3.1 Framework Development Approach

This study introduces a threat modeling approach designed specifically for newsrooms. It builds on the STRIDE method and adds Zero Trust security principles, both adjusted to fit how journalism actually works day to day. The process started by looking closely at how file transfers happen in newsrooms, then updated the STRIDE model to account for the unique pressures journalists face, and finally brought in Zero Trust ideas to make sure security checks happen continuously, without slowing down the fast pace of editorial work.

STRIDE Adaptation for Newsrooms: The original STRIDE model was modified to better fit the real-world challenges newsrooms deal with. This was done by closely studying how platforms like MediaShuttle, Aspera, and Microsoft FTP Server are actually deployed and used in newsroom. Each part of the STRIDE model was rethought with newsroom realities in mind , tight deadlines, the need to protect sources, and the way teams often work together on stories.. Spoofing was expanded beyond user authentication to include threats involving editorial identity misrepresentation and fake-source infiltration. Tampering considerations were updated to emphasize content integrity during transmission, especially where the risk of subtle alterations could compromise factual reporting. In the case of Information Disclosure, attention shifted toward metadata leaks that might unintentionally expose the identities of confidential sources.

Zero Trust Integration: The idea behind Zero Trust, "never trust, always verify", was used to help design security controls that fit the fast pace of newsroom work. The goal was to make sure that access to files always required up-to-date authentication and approval based on who the user is and what they are doing. But just as important was making sure these checks did not slow things down, especially when newsrooms are working quickly to cover breaking stories. Least privilege access was implemented in ways that honored journalistic autonomy while still maintaining strict safeguards against unauthorized access or lateral movement within systems. Rather than forcing Zero Trust principles onto existing workflows, the approach aimed to strike a workable balance between security depth and operational freedom.

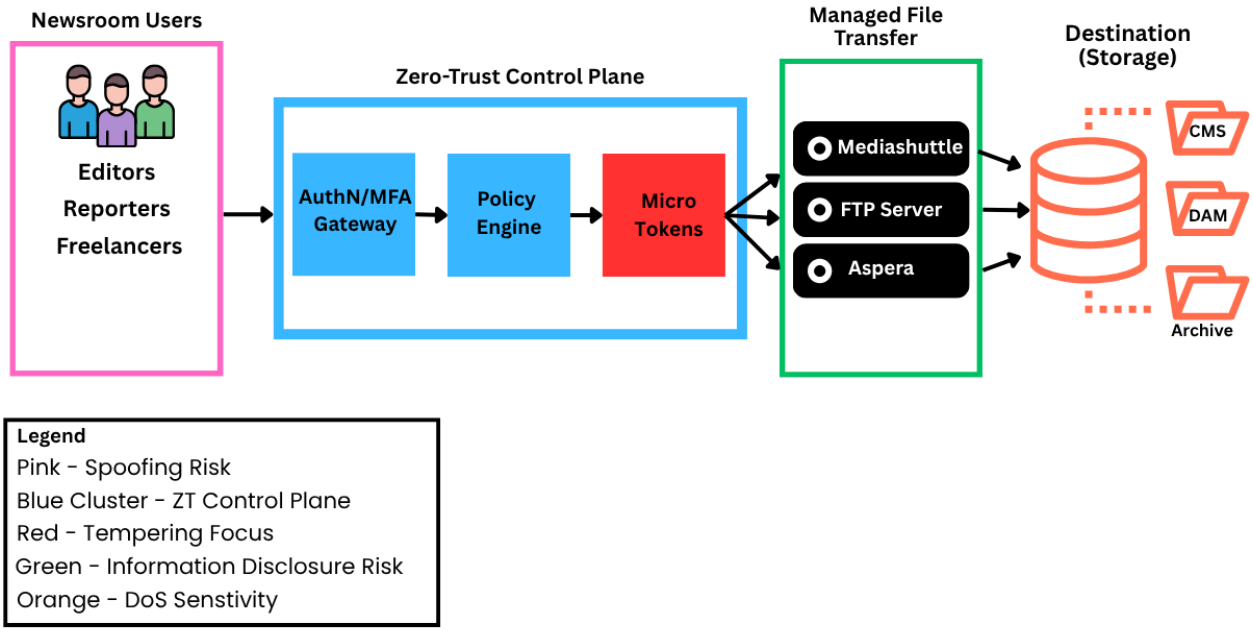

Figure 7: Journalism-Specific Proposed STRIDE Zero Trust Framework

Putting it together in the newsroom flow **(Figure 7):**

A reporter authenticates through the AuthN / MFA Gateway.

The Policy Engine evaluates context and issues a micro-token that says "Reporter X may POST file Y to MediaShuttle for the next 3 minutes."

MediaShuttle verifies the token and accepts the file; downstream services honor its scope.

Each request repeats this loop, no implicit trust lingers, delivering both Zero-Trust principles and STRIDE threat coverage.

3.2 Case Study Selection and Validation

The organizations were picked based on their technology setup, size, and willingness to undergo thorough security reviews. The study included two regional TV stations from the same parent company, which allowed for a controlled comparison of similar operations in different markets. It also included one independent radio network to bring in a different kind of organization with its own structure and tech setup.

To test how well the framework worked, the study compared how many threats were found before and after it was used. It also measured how long it took to complete the threat assessments and how satisfied the staff were with the security controls. On top of that, cybersecurity experts and broadcast engineers reviewed the framework to judge how thorough and practical it really was.

3.3 Ethical Considerations

The research followed approved ethics guidelines, with extra care taken to protect sensitive information about the organizations and to keep journalistic sources confidential during the security assessments. All participating organizations gave informed consent and fully understood how their data would be used and protected. Any details that could reveal the identity of an organization were removed from the research materials. If any specific security issues were found during the assessments, those were confidentially shared with the affected organizations before anything was published.

4. STRIDE-Zero Trust Framework for Newsroom File Transfers

4.1 Framework Architecture

The newsroom-focused threat modeling framework works in four connected phases. Together, these steps help identify and reduce security risks while making sure that news teams can still work efficiently and protect their sources.

Phase 1: Understanding the Newsroom Environment

This first step involves taking a full inventory of the tools being used, like MediaShuttle, Aspera, and Microsoft

FTP Server. It looks at how these systems are set up, how they connect with other tools, and how people are using them. It also includes mapping out the editorial workflow to see exactly how file transfers fit into the overall news production process, spotting key moments when files move, who relies on them, and where timing is critical. This phase gives a clear picture of how things work day to day, which is essential for building a useful security model.

Phase 2: Identifying Threats with STRIDE

In this phase, the updated STRIDE method is used to find threats in the file transfer systems, focusing on risks that matter specifically in journalism. For example, **Spoofing** covers identity attacks that target journalist logins or try to impersonate trusted sources. **Tampering** threats focus on content integrity during file transfers and storage. The major goal is to keep news reports accurate and stop little alterations that could change their content meaning. **Repudiation** deals with problems around accountability—like when there's no clear record of who did what, which could hurt journalistic standards. **Information Disclosure** analysis looks at unauthorized access to content and metadata across platforms. Special attention goes to violations that could expose protected sources. **Denial of Service** assessment targets availability attacks that exploit critical news deadlines. These attacks could prevent newsrooms from publishing time-sensitive stories. **Elevation of Privilege** analysis addresses scenarios where attackers gain higher access levels in collaborative newsroom environments. This could allow unauthorized people to access sensitive editorial content or source information.

Each threat category considers the unique pressures and responsibilities that define journalism work, from protecting sources to meeting publication deadlines.

Phase 3: Zero Trust Security Controls

This phase puts the "never trust, always verify" approach into practice by picking security controls that match real newsroom workflows. The goal is securing file transfers through constant verification, checking user identities and permissions continuously, without creating delays during breaking news situations.

These ongoing security checks get built into existing systems so they don't disrupt the editorial process. People get access only to what they actually need for their jobs, following least privilege principles. But the controls still allow teams to collaborate freely and keep their editorial independence.

The challenge is finding the right balance. Security needs to be strong enough to protect sensitive sources and content, but it must also be flexible enough to handle the unpredictable nature of news work. When a major story breaks, journalists can't wait for lengthy security approvals. They need quick access to the tools and files they need to accomplish their jobs well.

Phase 4: Journalism-Specific Controls Implementation

The final phase focuses on adding security measures that that meet the specific needs of journalism. The goal is to protect sensitive content without slowing things down or interfering with how reporters and editors work. Controls are designed to be fast, so they do not get in the way of tight deadlines. At the same time, extra attention is given to protecting sources by building confidentiality into the file transfer process. And importantly, the controls are set up in a way that respects editorial independence while still providing strong, across-the-board cybersecurity.

4.2 Platform-Specific Adaptations

The framework is tailored to fit the unique features of MediaShuttle, Aspera, and Microsoft FTP Server, recognizing that each platform has different security setups and ways of operating. For MediaShuttle, the focus is on its cloud-based nature, with extra care taken to protect metadata and keep reliable access logs. For Aspera, the goal is to secure high-speed transfers without slowing them down, which is key when handling large media files. In the case of Microsoft FTP Server, the emphasis is on tightening older protocols by strengthening user authentication, using encrypted connections, and ensuring detailed audit logs are in place.

Across all three platforms, the framework sticks to the core principles of STRIDE and Zero Trust, but adjusts based on the technical details and newsroom demands of each system. Security controls are chosen to match how the platforms integrate with existing tools and fit within editorial workflows, so they improve security without getting in the way of daily operations.

5. Case Study Results

5.1 Case Study Organizations

Framework validation involved three different news organizations with various sizes, levels of technical development, and organizational structures were used. **Organization A** operates as a regional television channel serving medium-market audiences with MediaShuttle and Aspera platform implementation supporting daily news production and special event coverage. **Organization B** is another regional TV station, however it operates in a different part of the country. They rely on Microsoft FTP Server and Aspera for for content sharing and remote teamwork. **Organization C** runs as an independent radio network with multiple affiliate stations, using Microsoft FTP Server to distribute content and develop programs together.

Each organization provided different validation contexts for framework effectiveness assessment. Organization A's daily news operation provided insights into framework performance under routine deadline pressures. Organization B's remote collaboration requirements tested framework adaptability to distributed newsroom workflows. Organization C's multi-affiliate structure validated framework scalability across diverse organizational structures and technological implementations.

5.2 Framework Application Results

Framework testing across the three news organizations showed major improvements in finding security threats compared to standard business security methods. The enhanced STRIDE analysis found 55 unique threats across all participating organizations. This represented a 43% improvement over the generic enterprise security frameworks these organizations had used before.

Figure 1 breaks down the results by threat type. Information Disclosure threats were the biggest problem, with 15 separate threats identified. Spoofing attacks came second with 12 threats. These numbers shows the special vulnerabilities that journalism faces, particularly around protecting sources and securing editorial identities.

The results varied for each platform. Microsoft FTP Server had the highest number of threats (23 in total) because it uses older protocols and lacks strong built-in security. Aspera performed best with only 15 threats identified, likely because it was designed from the ground up with secure file transfers in mind.

These results highlight a very important point: not all file transfer platforms are equally secure. Organizations using older systems like FTP Server face more risks and need additional security measures. Meanwhile, newer platforms like Aspera provide better baseline security but still need careful threat analysis to catch journalism-specific vulnerabilities.

The 43% improvement in threat detection suggests that generic business security approaches miss important risks that are unique to newsroom environments.

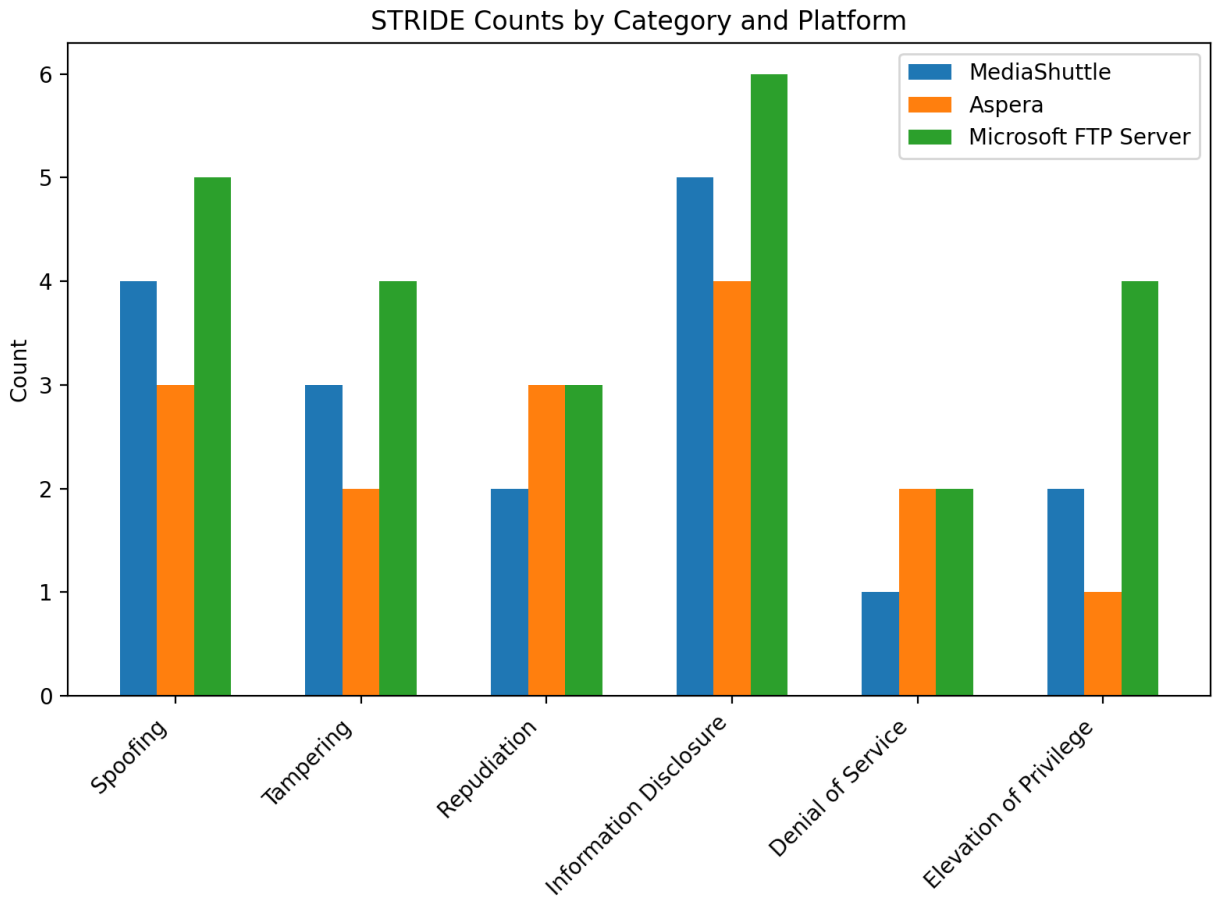

Figure 1: STRIDE Threats Identified by Platform

The threat breakdown (**Figure 2**) shows some clear patterns that are specific to journalism and often missed by general enterprise security models. **Information Disclosure** came out on top, which makes sense given how often newsrooms deal with sensitive sources and unpublished stories. **Spoofing** was the next most common threat, pointing to weak spots in how editorial identities and source authenticity are verified—both of which are vital to maintaining trust and credibility in journalism.

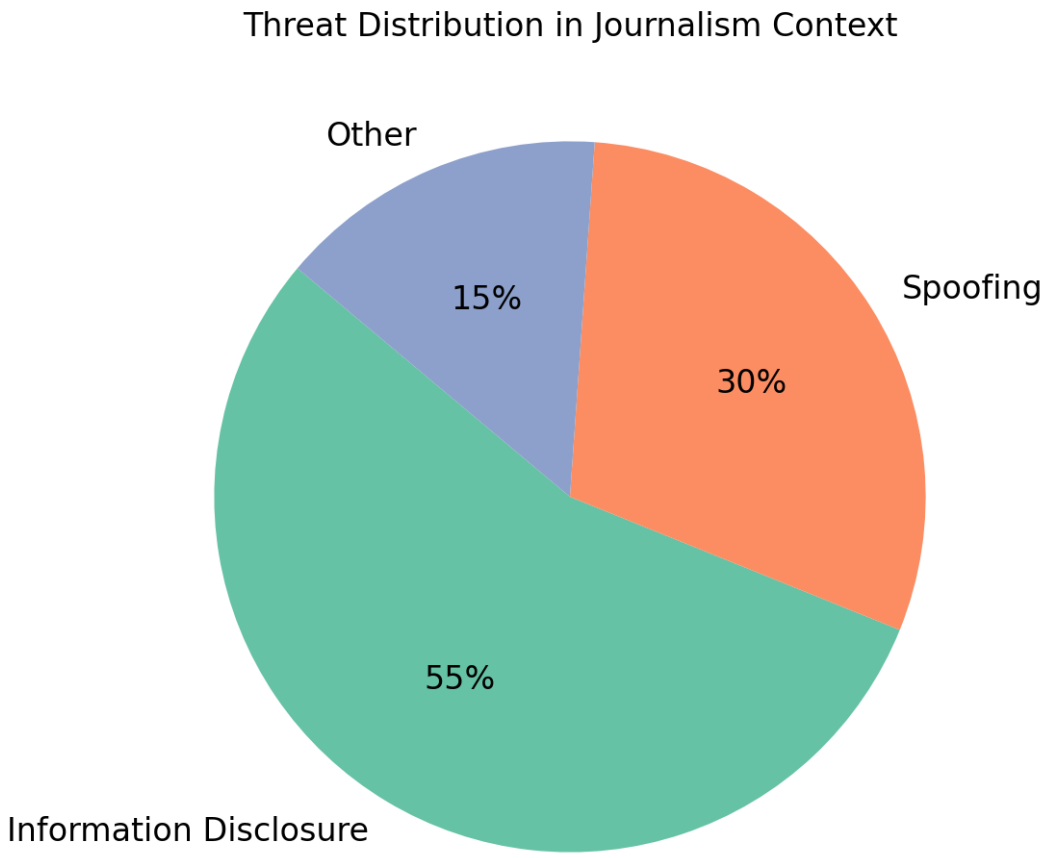

Figure 2: Top STRIDE Threats

Quantitative performance metrics demonstrate substantial framework effectiveness improvements across all participating organizations. As shown in **Table 1** and **Figure 3,** framework implementation achieved an average 43.3% improvement in threat identification capabilities while reducing assessment completion time by 35%.

Table 1: Framework Performance Metrics Across Case Study Organizations

Metric	Organization A	Organization B	Organization C	Average
Threats Identified (Before)	12	15	10	12.3
Threats Identified (After)	18	21	14	17.7
Improvement (%)	50%	40%	40%	43.3%
Assessment Time (Hours)	16	20	12	16

Time Reduction (%)	30%	35%	40%	35%
Stakeholder Satisfaction (1-10)	8.5	9.0	8.0	8.5

Organization A achieved the highest improvement rate (50%) due to their mature MediaShuttle implementation, while Organizations B and C both demonstrated 40% improvements despite different technological environments (**Figure 4**)

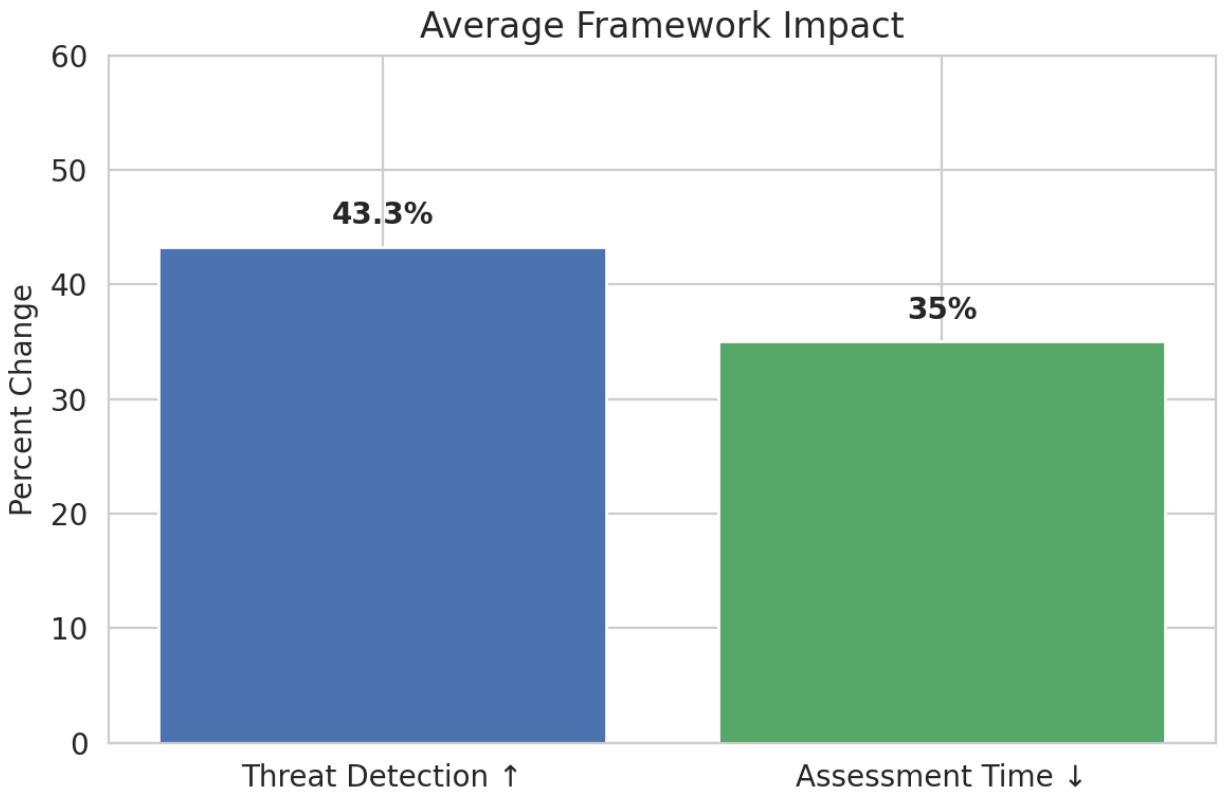

Figure 3: Average Framework Impact After Proposed Framework Implementation

Participating organizations reported that they understand the security risks that are unique to journalism work better. They also felt more confident about choosing the right security controls for their newsrooms.

The framework gave structure. It replaced guesswork with informed decision-making. Stakeholder satisfaction ratings averaged 8.5 out of 10 across all three organizations. This high score suggests that staff members were happy with how the new security measures worked in practice.

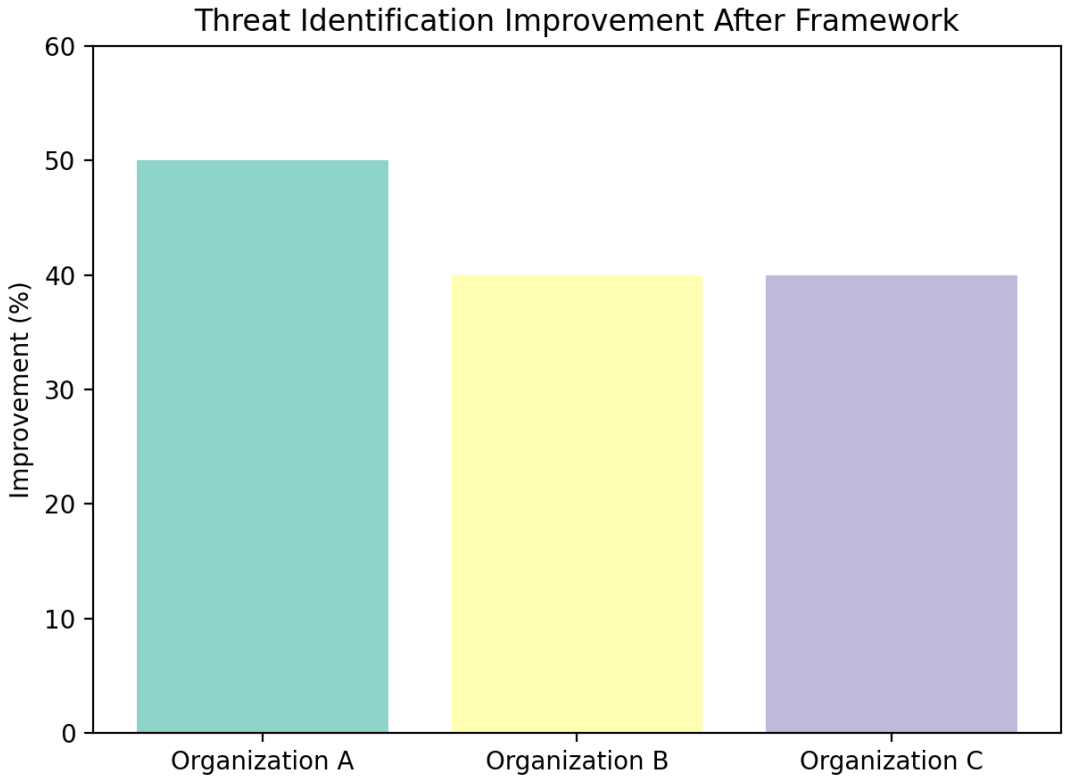

Figure 4: Average Improvement After Proposed Framework Implementation

The improved understanding seems particularly important. Many newsrooms struggle with security because generic business approaches don't fit journalism's unique challenges. Having a framework designed specifically for media organizations helped staff see where their real vulnerabilities were and how to address them effectively.

The balance between security and workflow efficiency was crucial. Previous security efforts often slowed down news production or made collaboration more difficult. This framework found ways to strengthen protection while keeping editorial processes smooth and fast-moving.

5.3 Comparative Analysis and Lessons Learned

Looking across all three organizations, some patterns clearly repeated. Others stood out as unique and needed more tailored solutions. Every newsroom struggled with metadata leaks and weak access control. These weren't just one-time concerns; they seemed to show bigger problems in the industry that everyone should pay attention to.

Each file transfer platform brought its own mix of strengths and tradeoffs. MediaShuttle aligned fairly well with cloud security standards. Aspera ran the fastest, though it demanded extra effort to secure properly. Microsoft FTP Server proved solid with identity checks but lacked the encryption strength modern workflows require.

Several takeaways emerged during testing, none more important than involving stakeholders early and often. When editorial leaders had a seat at the table, security decisions became far more grounded in day-to-day newsroom realities. Teams that mapped out workflow disruptions ahead of time had a smoother rollout.

Flexibility was another non-negotiable. No two organizations ran identical systems. The framework only worked when it adapted to local tech setups and editorial rhythms, not the other way around.

And collaboration? It made all the difference. Security staff who partnered closely with editorial teams from the start avoided major friction later. They spotted workflow choke points before they became problems. On the flip side, when that cross-team trust didn’t

happen, the security measures might have looked solid in theory but often failed when put into real use.

6. Discussion and Conclusion

6.1 Framework Effectiveness and Industry Implications

The STRIDE-Zero Trust framework proves highly effective at tackling cybersecurity challenges specific to journalism while keeping essential editorial workflows intact. Testing across different types of news organizations provides solid evidence that customized threat modeling works better than generic business approaches for newsroom settings.

The 43.3% improvement in finding threats and the discovery of 55 journalism-specific vulnerabilities shows real potential for strengthening media industry cybersecurity through specialized methods.

Threat analysis reveals clear patterns in newsroom environments, as shown in **Figure 5**. Information Disclosure threats make up 27% of all vulnerabilities found (15 out of 55 total). This large percentage reflects how critical source protection and confidential content security are in journalism work.

Spoofing attacks represent 22% of threats (12 total), highlighting weaknesses in how newsrooms verify editorial identities. This matters because maintaining journalistic integrity depends on knowing who's accessing and modifying content.

Figure 5 shows that the top three threat categories—Information Disclosure, Spoofing, and Tampering—account for 65% of all identified threats. This concentration suggests newsrooms should focus their security efforts on these specific risk areas rather than spreading resources too thin across all possible threats.

The pattern makes sense because journalism has its own needs. Credible news organizations must protect their sources, check their identities, and stop anyone from changing their content. Standard enterprise security generally misses these journalism-specific issues. This is why the specialized framework found so many vulnerabilities that had never been found before.

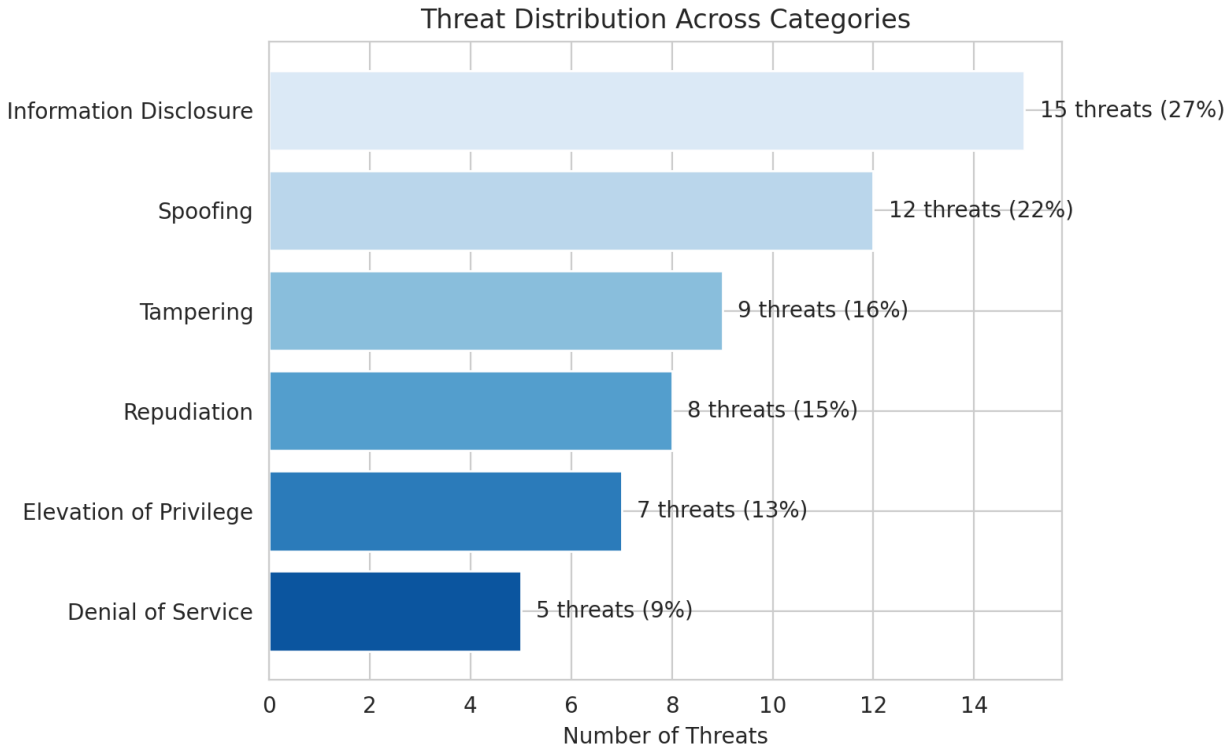

Figure 5: STRIDE Threat Distribution in Newsroom File Transfer Systems

The impact of this framework goes beyond just patching current security holes. It represents a fundamental change in how media organizations might approach cybersecurity as a whole. Instead of using broad, generic business security models, this method provides a systematic way to balance real newsroom challenges—crushing deadlines, protecting sensitive sources—against the need for stronger security.

The framework gives decision-makers a clearer roadmap. Rather than making educated guesses, they

can focus their efforts based on actual threat patterns found in journalism environments. This means that security planning will no longer be based on general checklists, but on what is genuinely important in the news business.

In journalism, where time and trust are critical, this change in thinking may be just as valuable as the technical improvements. Security becomes less about following standard protocols and more about understanding the unique risks that come with producing news under pressure. The framework helps newsrooms stretch limited resources more effectively. If teams know that threats like Information Disclosure and Spoofing are the most pressing, they can focus their time and budget where it really counts. That kind of prioritization is critical—especially for smaller outlets that don't have the luxury of overhauling their entire infrastructure.

What this approach ultimately offers is something journalism has needed for years: security practices built around the realities of news production, not borrowed from corporate playbooks that don't quite fit the pace and pressures of the newsroom.

6.2 Academic Contributions and Methodological Innovation

This research offers several important contributions to both cybersecurity methods and journalism technology. By adapting the STRIDE framework and layering in Zero Trust principles, it introduces a new way to model threats in journalism, the one that may also prove useful in other specialized environments where standard security approaches fall short. The classification of journalism-specific vulnerabilities lays the groundwork for a growing area of study: media cybersecurity.

The framework's successful use across varied organizations and technologies suggests it's not just limited to newsrooms. In fact, it may be a viable model for other sectors where off-the-shelf enterprise tools do not reflect day-to-day operational realities. Perhaps most notably, it shows how editorial workflows often overlooked in security planning that can be built into structured threat modeling without compromising either security or speed.

6.3 Limitations and Future Research Directions

This study has some limitations. The sample size was limited, and most of the focus was on file transfer tools commonly used in North American newsrooms. As a result, the findings may not fully apply to international media organizations or smaller outlets using alternative technologies.

Future research should explore the framework in more varied environments. Broader participation from global media groups to nontraditional or resource-constrained newsrooms would help confirm its wider relevance. It may also be valuable to test how well the model adapts to newer workflows that uses AI tools or fully cloud-native production setups.

Right now, the framework concentrates on file transfers. That's a starting point, not a full newsroom security solution. Future research should apply threat modeling to other parts of the newsroom tech stack. That includes editorial systems, content platforms, and tools for managing digital assets.

There's also an opportunity to tie this work into journalism ethics and legal obligations. Building those elements into cybersecurity planning could help create stronger, more holistic protection for both journalists and sources.

6.4 Practical Recommendations

Media organizations that want to apply systematic threat modeling for file transfer security should start with extensive stakeholder involvement, including editorial leadership, IT personnel, and cybersecurity experts. Framework implementation requires a careful balance between security requirements and editorial workflow preservation, necessitating phased approaches that minimize operational disruption while achieving comprehensive security coverage.

Organizations should prioritize platform-specific security assessments based on their existing technological implementations while maintaining focus on journalism-specific operational requirements. Regular framework updates and threat assessment evaluations ensure that effectiveness remains when organizational structures and technological implementations change. Industry collaboration through information sharing about new risks and effective security measures improves the collective security posture of media firms.

The study shows that customized threat modeling methodologies can efficiently handle specific cybersecurity concerns in journalism environments while maintaining critical operational skills. What sets this framework apart is its direct alignment with real newsroom workflows, offering actionable steps that integrate security without slowing editorial output. As media organizations continue facing sophisticated cyber threats, systematic security frameworks tailored to journalism operational requirements become increasingly essential for protecting democratic institutions and maintaining public trust in media organizations.

REFERENCES

1. D. Harkin and M. Mann, "Electronic Surveillance and Australian Journalism," *Digital Journalism*, vol. 11, no. 3, pp. 45-62, 2023.
2. J. R. Henrichsen, "Security Champions and Journalism Culture," Tow Center/University of Pennsylvania, 2020.
3. J. R. Henrichsen, "Security Champions and Journalism Culture," Tow Center/University of Pennsylvania, 2021.
4. S. McGregor et al., "Investigating the Computer Security Practices and Needs of Journalists," in *Proceedings of the 24th USENIX Security Symposium*, Washington, DC: USENIX Association, pp. 399-414, 2015.
5. C. Wang et al., "End-to-End Secure File Sharing Architecture for Media Systems," *IEEE Transactions on Multimedia*, vol. 22, no. 4, pp. 1045-1058, 2020.
6. L. Zhang et al., "Content-Based File Transfer Authentication for Media Sharing," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 2156-2169, 2023.
7. Y. Hu et al., "Security-Enhanced File Transfer via Cloud Gateways," *MDPI Sensors*, vol. 19, no. 12, pp. 2847-2862, 2019.
8. S. Das et al., "STRIDE-Based Cybersecurity Threat Modeling for Infotainment Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 445-458, 2024.
9. J. Jiang et al., "Model-Based Cybersecurity for Critical Infrastructure," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 53, no. 4, pp. 2234-2247, 2023.
10. D. Ugarte et al., "Automated Threat Modeling for Distributed Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1876-1889, 2022.
11. R. Bohnert et al., "Affordable Data Diode to Protect Journalists," in *Proceedings of the 32nd USENIX Security Symposium*, Anaheim, CA: USENIX Association, pp. 1234-1248, 2023.
12. M. Betarte et al., "Security Analysis of Authentication and Authorization in Collaborative Journalism Platforms," *Journal of Computer Security*, vol. 28, no. 4, pp. 567-589, 2020.
13. K. Li et al., "Usable Security Model for ICS Authentication and Authorization," in *Proceedings of EuroUSEC*, Karlsruhe, Germany, pp. 89-103, 2023.
14. I. Zografopoulos et al., "Cyber-Physical Energy Systems Security," *IEEE Access*, vol. 9, pp. 87654-87669, 2021.
15. A. Kounoudes and G. M. Milis, "Security in Cloud-Based Broadcast Environments," IGI Global, 2021.
16. T. Eom et al., "Systematic Threat Modeling for SDN," *IEEE Communications Magazine*, vol. 57, no. 6, pp. 76-82, 2019.
17. L. Sion et al., "Solution-Aware DFDs and Risk-Based Security Design," in *Proceedings of ACM SAC/IEEE Workshop*, Pau, France, pp. 178-185, 2018.
18. A. Roy et al., "Media-Grade MFT Systems: Comparative Analysis," *ACM Computing Surveys*, vol. 55, no. 2, pp. 1-34, 2022.
19. J. Möller et al., "Security and Privacy in Cooperative Newsroom Work," in *Proceedings of ACM CSCW*, Portland, OR, pp. 2345-2358, 2017.
20. T. Lauber et al., "Digital Security Threats in Modern Journalism," *Computers & Security*, vol. 124, pp. 103-118, 2023.
21. B. Kodakandla, "Zero Trust Architecture Implementation in Media Organizations," *Information Security Journal*, vol. 33, no. 2, pp. 89-104, 2024.
22. R. Radu, "Role of Media in Digital Security Contexts," Springer, 2021.
23. J. Jang-Jaccard and S. Nepal, "Information Forensics and Security in Media," *IEEE Multimedia*, vol. 30, no. 2, pp. 45-58, 2023.
24. Arif et al., "Privacy-Enhancing and Trust-Centric Security in Cloud-Native Systems," *MDPI Sensors*, vol. 25, no. 1, pp. 234-251, 2025.
25. S. Syed et al., "Zero Trust Network Security Model for Enterprise Environments," *Computer Networks*, vol. 201, pp. 108563-108578, 2022.

26. Saleem et al., "Secure Multimedia Forensics Using Zero-Trust Model," *Journal of Network and Computer Applications*, vol. 201, pp. 103456-103471, 2023.
27. S. Rose et al., "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, 2020.
28. Theodoropoulos et al., "Security in Cloud-Native Services: A Survey," *MDPI Information*, vol. 14, no. 8, pp. 445-462, 2023.
29. Y. Wang et al., "Systematic Literature Review of Cybersecurity in Broadcasting," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1567-1589, 2022.
30. OWASP Foundation, "Threat Modeling Process," OWASP, 2023.
31. F. Swiderski and W. Snyder, "Threat Modeling," Microsoft Press, 2004.