Where Is Cybersecurity? An Analysis of U.S. State Hazard Mitigation and Emergency Plans

Kendel Woodburn
Brigham Young University
klw254@byu.edu

Shydra Murray
Brigham Young University
shywilli@byu.edu

Amanda Lee Hughes
Brigham Young University
amanda_hughes@byu.edu

ABSTRACT

Despite the growing convergence of physical and cyber risks, U.S. state disaster planning remains uneven in its treatment of cybersecurity threats. While federal guidance promotes an all-hazards approach to preparedness, the extent to which state-level hazard mitigation and emergency plans address cyber risks has not been systematically characterized. We present a national assessment of cybersecurity content in State Hazard Mitigation Plans (SHMPs: all 50 states) and State Emergency Plans (SEPs: 45 states). Using content analysis, we examine cyber risk framing, coverage across the emergency management cycle, and governance mechanisms (responsibilities, standards, detection, reporting). Although many plans reference cybersecurity, coverage varies widely and is often limited for recovery/continuity, threat detection, and procedural reporting guidance. SHMPs emphasize risk identification and mitigation, while SEPs emphasize agency roles and response coordination. We discuss implications for cyber crisis governance and identify practical priorities for strengthening state planning and supporting more coordinated cyber disaster readiness.

Keywords

Cybersecurity, Disaster Resilience, Hazard Mitigation Planning, Emergency Management, Critical Infrastructure.

INTRODUCTION

Cybersecurity has become an important component of national resilience, as governments and critical infrastructure operators face an increasing number of cyber threats with the potential to disrupt services, compromise sensitive information, and undermine public trust. In 2023, ransomware attacks surged globally, with reported incidents rising 73% from the previous year (Grossman & Smith, 2024). Yet much of the cybersecurity literature and practice guidance focuses on securing systems under "steady state" conditions (e.g., enterprise risk management, compliance, and routine incident response). We have far less visibility into how cyber risks are incorporated into the plans that guide multi-actor crisis response and recovery, where uncertainty is high, coordination is distributed, and operational authority is often shared across organizations and jurisdictions.

This gap is particularly salient given the increasing convergence of cyber and physical hazards. As Panda and Bower (2020) argue, cybersecurity risks and cascading effects should be recognized as part of an all-hazards approach to disaster resilience. Cyberattacks frequently occur during or in the wake of natural disasters, when infrastructure is degraded and institutional vulnerabilities are heightened (Chakraborty et al., 2024; Radianti, 2025). In the United States (U.S.), the number of federally declared major disasters has grown significantly, increasing by over 60% between the late 1980s to the most recent decade studied, driven by more frequent and

severe disasters, climate change, and development in hazard-prone areas (Lee et al., 2025). As emergency management grows more reliant on digital infrastructure, the resilience of those systems becomes critical to effective disaster response.

In the U.S., federal policy and guidance require states to engage in planning across multiple domains. Under the Disaster Mitigation Act of 2000 (DMA 2000), all U.S. states must develop and maintain an approved State Hazard Mitigation Plan (SHMP) to be eligible for federal disaster funding through programs administered by the Federal Emergency Management Agency (FEMA). In parallel, most states also maintain a State Emergency Plan (SEP), developed in accordance with FEMA guidance and federal expectations under the Stafford Act of 1988, to support coordinated disaster response and recovery efforts. These documents are, in effect, governance artifacts. They specify responsibilities, coordination structures, and mechanisms for communication and learning across agencies and sectors.

Yet, it remains unclear how extensively cybersecurity has been integrated into these planning documents. Prior research has shown significant variability in the quality and scope of state hazard mitigation plans (Frazier et al., 2013; Habets et al., 2024). FEMA provides guidance for required elements in plans, but it leaves considerable discretion to states in how they address emerging risks such as cybersecurity. Furthermore, cybersecurity and emergency management have developed along separate policy and institutional trajectories, potentially leading to inconsistencies in how cyber risks are addressed in disaster planning.

To address this gap, we systematically collected emergency and hazard mitigation plans from all 50 U.S. states and analyzed them using qualitative content analysis. We examine the extent and nature of cybersecurity content in these documents, identify cross-state patterns and disparities, and highlight examples of more comprehensive integration. In doing so, we contribute to ongoing scholarly and policy conversations around building more cyber-resilient emergency management systems.

BACKGROUND

While hazard mitigation planning in the U.S. has received scholarly attention, most studies have focused on "traditional" threats such as floods, earthquakes, or hurricanes. Prior work has documented variation in how states identify risks, assess vulnerabilities, and comply with federal planning requirements. For example, Lyles et al. (2014) examined disparities in local plan quality and emphasized the influence of state-level mandates on shaping outcomes. More recently, Habets et al. (2024) evaluated SHMPs across all 50 states. They identified significant inconsistencies in how plans incorporate social vulnerability indicators and conduct risk assessments, even when formally compliant with FEMA guidelines.

In contrast, cybersecurity has been less consistently examined within the hazard mitigation and emergency planning literature (Radianti, 2025). FEMA's framework provides general structure for SHMPs and encourages states to address a range of hazards, but it offers limited guidance on how to integrate cyber risks. This lack of guidance reflects broader global challenges. Panda and Bower (2020) note that national and local disaster risk reduction plans worldwide have yet to meaningfully incorporate cyber resilience, despite growing awareness of interconnected and cascading risks. In the U.S. context, this limited guidance means that states retain wide discretion in how—and whether—to include cybersecurity in their planning efforts. Gall et al. (2024), in a close examination of Louisiana's plans, found that even when non-traditional risks are acknowledged, they are rarely integrated into a cohesive strategy.

In parallel, research on cybersecurity in crisis contexts has shown why this planning question matters. Cyber incidents often coincide with—or follow—physical disasters and target critical systems during moments of disruption (Chakraborty et al., 2024; Kishi et al., 2017). Yet many public sector organizations, particularly at the state and local levels, lack dedicated cybersecurity capacity and instead rely on third-party support (Groenendaal et al., 2022). These challenges have become more visible following the COVID-19 pandemic and amid rising geopolitical tensions, both of which have accelerated digital dependence and exposed gaps in resilience (Ganapati et al., 2023; Lawson & Tobey, 2022; Lee et al., 2024; Lindström et al., 2024).

This prior work motivates the question: how are U.S. states incorporating cybersecurity into the planning documents that guide mitigation, response, and recovery? To answer this, we systematically analyze SHMPs and SEPs from all 50 U.S. states. We aim to provide a clearer picture of how cyber risks are—or are not—being incorporated into state-level emergency and mitigation planning.

METHODS

Data Collection

To assess how cybersecurity is incorporated into state-level disaster planning, we compiled a corpus of two core

types of planning documents: State Hazard Mitigation Plans (SHMPs) and State Emergency Plans (SEPs). SHMPs were defined as plans submitted for FEMA review as part of the state's hazard mitigation planning process. SEPs were defined as publicly available, state-level response and recovery plans intended to guide coordinated emergency operations (including documents titled *Emergency Operations Plan*, *Emergency Management Plan*, *Emergency Response Plan*, or similar).

We identified documents through systematic searches of official state government and emergency management agency websites. For each state, we (1) navigated to the state emergency management agency's website (or equivalent homeland security / emergency services site) and searched for planning documents, and (2) conducted targeted site searches using combinations of keywords such as: state hazard mitigation plan, SHMP, emergency plan, emergency operations plan, EOP, state emergency plan, emergency management plan, and disaster response plan. When multiple versions were available, we selected the most recently posted plan at the time of collection. The location of SHMPs and SEPs varied by state: some were found on emergency management pages, while others were hosted on homeland security pages. File formats also differed, with some plans available as PDFs, others as text documents, and some only presented as information on a webpage with no download option. This lack of a consistent publication standard across the U.S. made these documents difficult to identify systematically.

We located SHMPs for all 50 states. SEPs were more difficult to identify, as not all states provide a current version online. We were unable to locate a publicly available SEP for 5 states: Delaware, Iowa, Minnesota, Missouri, and Wyoming. This does not necessarily indicate that such plans do not exist, only that they were not accessible through public sources or could not be located at the time of data collection. All collected documents were downloaded and imported into Dovetail, a qualitative data analysis platform, to support systematic document management and coding.

Table 1. Coding framework used to identify cybersecurity-related content in state hazard mitigation plans (SHMPs) and state emergency plans (SEPs)

Category	Subcategories	Definition
Cyber Risk Context	Overview	Introductory or orienting statements that frame the purpose, scope, or placement of cybersecurity within the plan, without specifying concrete operational actions, assigned responsibilities, or incident procedures.
	Definitions	Explanation of cybersecurity terms and concepts.
	Cyber Risks	Description of potential cyber attacks, vulnerabilities, and associated risks.
	Impact	Potential impacts of cybersecurity incidents.
	Hazard History	Historical record of prior cyber attacks or incidents.
	Future Probability	Assessment of likelihood of future cyber attacks.
Cyber Disaster Management Cycle	Mitigation	Actions to reduce the likelihood or impact of cybersecurity incidents.
	Response	Actions to address an active or recently identified cybersecurity incident.
	Recovery	Actions to restore normal operations after a cybersecurity incident.
	Preparedness	Efforts to prepare for cybersecurity incidents, including planning, training, and coordination.
Cyber Policies & Procedures	Agency Responsibilities	Defined roles and responsibilities of agencies involved in cybersecurity response.
	Standards	Information and technology standards established to support continuity of state operations.
	Strategies	Strategic plans to enhance protection against cyber incidents.
	Threat Detection	Detection actions to identify cybersecurity incidents.
	Reporting	Processes for notifying relevant authorities about cybersecurity incidents.

Coding Framework

We developed a structured coding framework to capture the ways in which cybersecurity is represented in state-level emergency and hazard mitigation plans. An initial review of a subset of documents informed a preliminary coding scheme consistent with qualitative content analysis (Schreier, 2012; Krippendorff, 2019). The framework was then refined through iterative team discussions.

The final framework (see Table 1) includes three broad categories. The first category, *Cyber Risk Context*, captures how cybersecurity risks are defined, contextualized, and assessed as hazards in the plans. The second, *Cyber Disaster Management Cycle*, focuses on how plans address cybersecurity across the four phases of emergency management: preparedness, mitigation, response, and recovery. The third, *Cyber Policies & Procedures*, captures governance structures, operational protocols, and detection and reporting processes related to cybersecurity.

Coding & Analysis

Two researchers applied the coding framework across the corpus using an iterative coding process that combined independent coding with regular adjudication meetings. Before full-corpus coding, the two coders jointly reviewed a small set of plans to align on how the codebook would be applied in practice, working through examples and edge cases and refining code definitions. The unit of coding was a text segment (typically a sentence or short paragraph) expressing a single idea relevant to a subcategory.

Text segments were coded to capture both explicit mentions of cybersecurity and references embedded in broader discussions (e.g., critical infrastructure protection, IT continuity, emergency communications, or interagency coordination). This approach was designed to capture both direct and indirect representations of cybersecurity planning. As a result, a single plan could contain multiple segments coded to the same subcategory, and segments ranged from brief mentions of cybersecurity to more detailed explanations of cybersecurity concepts.

During coding, we held weekly meetings to discuss ambiguous segments and resolve disagreements through consensus. When a segment could plausibly fit more than one subcategory, coders assigned the single most specific applicable code based on the finalized code definitions. We also revisited and re-coded early documents after finalizing the codebook to ensure consistent application across the corpus.

As a targeted check on coding consistency, we conducted a post hoc validation on a subset of coded excerpts using the finalized codebook. Because relevant segments varied in length and were not treated as fixed, pre-segmented units, this validation focused on agreement in code assignment for selected excerpts rather than on independent identification of text boundaries. A third coder independently assigned the single best-fitting subcategory to 100 segments randomly sampled from both SHMPs and SEPs. Agreement between the third coder's assignments and the finalized study coding was high, with Cohen's kappa = 0.94 and 95% agreement. This check complemented the study's original consensus-based coding process.

The resulting coded dataset supports descriptive summaries of cybersecurity-related content (e.g., plan-level presence of subcategories and counts of coded segments) and comparative analyses across plan types and states.

RESULTS: COVERAGE OF CYBERSECURITY IN STATE PLANS

Cybersecurity appeared in a majority of both state mitigation and emergency plans, though coverage varied substantially in scope and specificity. At the plan level, 70% of SHMPs and 84.4% of SEPs included at least some reference to cybersecurity. SEPs were more likely to address operational aspects of cybersecurity (e.g., agency responsibilities, response protocols), while SHMPs tended to emphasize risk identification and mitigation strategies.

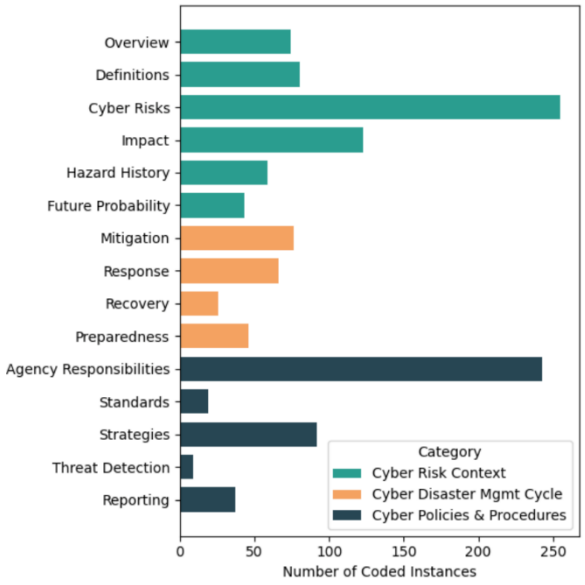

Figure 1. Number of coded text segments in each cybersecurity category and subcategory across all collected SHMPs and SEPs

Figure 1 summarizes cybersecurity content across our coding framework using coded instances (tagged text segments) rather than counts of plans. Because a single plan can contain multiple segments relevant to a given subcategory, instance counts reflect how often a topic appears in the corpus, not how many states address it. Several broad patterns are visible in the coded dataset.

The *Cyber Risk Context* category was the most consistently represented, particularly its subcategories *Cyber Risks*, *Impact*, and *Definitions*. This pattern indicates that many plans explicitly identify cybersecurity as a relevant hazard and outline its potential consequences, often by defining key terms and describing plausible impacts.

Coverage within the *Cyber Disaster Management Cycle* category was more uneven. While Mitigation and Response were often referenced, Recovery and Preparedness appeared less often. This imbalance reflects greater attention to response and mitigation activities than to longer-term resilience and planning efforts.

The *Cyber Policies & Procedures* category showed the greatest variability across states. The *Agency Responsibilities* subcategory was among the most frequently coded, reflecting efforts to clarify roles and responsibilities for cybersecurity coordination. In contrast, *Threat Detection*, *Standards*, and *Reporting* were sparsely represented. These results show that plans are more likely to specify responsible actors than to define detection and reporting procedures.

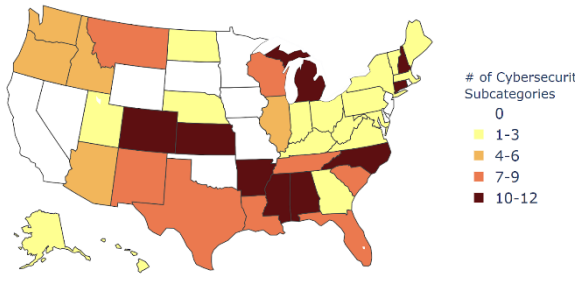

Figure 2. Number of cybersecurity subcategories represented in each SEP, based on at least one coded text segment per subcategory

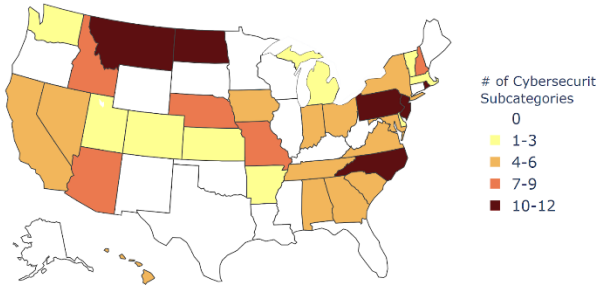

Figure 3. Number of cybersecurity subcategories represented in each SHMP, based on at least one coded text segment per subcategory

We then examined the extent to which state plans covered the 15 cybersecurity subcategories. Figures 2 and 3 visualize this distribution across emergency and mitigation plans, respectively. No plan covered all 15 subcategories. The most comprehensive plan covered 12 subcategories.

As shown in Figure 2, several SEPs (e.g., Connecticut, Kansas, and Michigan) referenced 11 or more subcategories, while a substantial number referenced fewer than five. Figure 3 shows the same analysis for SHMPs. Here, coverage was generally more uneven. A few states (e.g., North Dakota, Pennsylvania, and North Carolina) referenced a relatively large number of subcategories, but many SHMPs referenced only one or two.

These figures show that cybersecurity is visible in many state disaster plans, but the extent of integration remains uneven. A small subset of states address cybersecurity across a broad range of planning considerations, while many plans focus on a narrower set of elements—most commonly risk framing and general responsibilities—with less attention to detection, reporting, preparedness activities, and recovery/continuity.

RESULTS: CONTENT ANALYSIS OF CYBERSECURITY IN STATE PLANS

This section examines the qualitative content of cybersecurity-related material in state plans. We organize findings

around the three coding categories in Table 1: Cyber Risk Context, Cyber Disaster Management Cycle, and Cyber Policies & Procedures. For each subcategory, we report the number of plans in which the subcategory appears at least once (SHMPs, SEPs) and provide illustrative excerpts.

Cyber Risk Context

This category captures how state plans name and frame cybersecurity risks. It includes content that defines potential impacts, references past incidents, and assesses future risk.

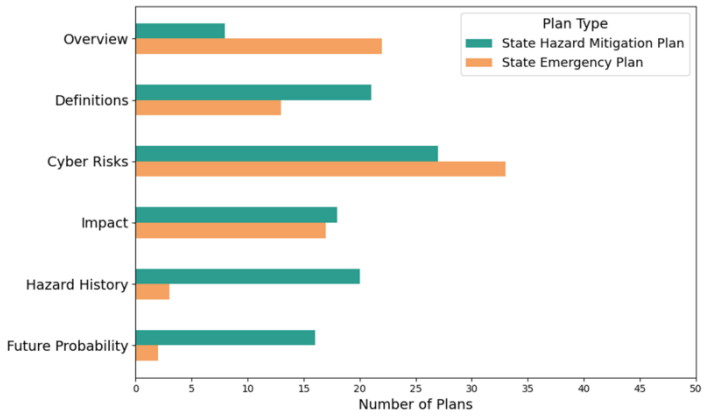

Figure 4. Number of SHMPs and SEPs containing at least one coded text segment in each Cyber Risk Context subcategory

Overview

(8 SHMPs, 22 SEPs). Most coded Overview passages summarized the purpose, scope, or structure of cybersecurity-related content in the plan. These statements often framed cybersecurity as a growing risk requiring coordinated attention. For example, North Carolina's emergency plan states: "*The purpose of this appendix is to establish a systematic approach for addressing a cybersecurity incident that affects or threatens to affect the citizens, economy, or government of North Carolina*" (NC, SEP)[1]. Some overview passages also stated broad planning objectives. Kansas' emergency plan, for instance, explains that "*An enduring goal of cyber defense is to either prevent or highly limit the contamination or damage of a system. But when that is not possible, the goal is to rapidly assess and implement action steps to limit the damage*" (KS, SEP). Several overview passages also situated cybersecurity within broader emergency support structures. Tennessee's emergency plan notes: "*Cyber Security ESF-17 coordinates support for cybersecurity-related incidents and can help identify subject matter expert resources for state and local government entities*" (TN, SEP). These overview passages position cyber incidents as an emergency management concern rather than solely an IT problem.

Definitions

(21 SHMPs, 13 SEPs). Definitions were common, especially in SHMPs, and were often used to establish shared terminology and signal alignment with authoritative sources. These Definitions commonly included general cybersecurity terms such as cybersecurity, cyberterrorism, cyberattacks, cyber incidents, and cyberspace. For example, North Dakota's mitigation plan cites NIST's[2] definition of cyberattack as "*any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself*" (ND, SHMP). Some plans also defined specific threat types. Pennsylvania's mitigation plan defines botnet as *"a collection of computers subject to control by an outside party, usually without the knowledge of the owners, using secretly installed software robots*" (PA, SHMP). The inclusion of Definitions ranged from basic glossaries to detailed technical explanations, reflecting variation in how plans present cybersecurity terminology to different audiences.

Cyber Risks

(27 SHMPs, 33 SEPs). Cyber Risks was the most frequently discussed topic across all plans, indicating that cybersecurity hazards were explicitly recognized in many documents. Many plans described common attack types. Connecticut's emergency plan, for example, notes that "*Cyber-attacks may take many forms: Destructive attacks, such as ransomware; Malware attempting to steal sensitive information; An uncontrolled exploit, such as a worm; Denial-of-Services,…*" (CT, SEP). Many plans included information about critical infrastructure most at risk. Rhode Island's hazard mitigation plan warns that disruptions could affect "*traffic control, dispatch, utility, and response systems*" as well as "*impact water or wastewater treatment facilities*" (RI, SHMP). However, the level of detail varied considerably across plans. Some provided only broad descriptions of cyber threats, while others offered more specific scenarios and sector-based risk profiles.

[1] Examples from state plans are cited using the state's two-letter U.S. postal code, followed by either SHMP for state hazard mitigation plans or SEP for state emergency plans.
[2] National Institute of Standards and Technology (NIST) – https://www.nist.gov

Impact

(18 SHMPs, 17 SEPs). The Impact subcategory captured instances where plans described the potential consequences of cybersecurity incidents. Many plans identified risks to infrastructure, economic stability, and public confidence. Connecticut's emergency plan states: "*Cyber incidents…can lead to disruptions in critical infrastructure, significant financial losses, and/or the theft of highly sensitive data*" (CT, SEP). Business continuity impacts were also noted. For instance, the North Dakota hazard mitigation plan states, "*...financial impact from ransomware attacks and downtime and recovery from a cyberattack can be damaging to the owners of properties, leading to abandonment from business closure*" (ND, SHMP). Some plans addressed effects on public trust, such as North Carolina's observation that "*Public confidence in the response of government organizations may be impacted by a cyber attack based upon societal expectations and media influence…There may be an expectation that government entities should do a better job of patrolling cyber crime*" (NC, SHMP). Across states, impact framing often appeared alongside broader recognition of cyber risk, even when procedural detail was limited elsewhere.

Hazard History

(20 SHMPs, 3 SEPs). The Hazard History subcategory was applied when a plan provided the history of previous attacks considered relevant to understanding the state's cyber risk. Many plans incorporated general statistics from FBI reports on cybercrime prevalence and financial losses. For example, Idaho's mitigation plan notes that "*In 2020, the State of Idaho ranked 38th in the United States for the number of cybercrime victims reported to the Internet Crime Complaint Center*" (ID, SHMP). Indiana's plan states that "*in 2021 alone… more than 11,000 Indiana residents were victims of cyberattacks totaling more than $60 million in losses*" (IN, SHMP). Some plans provided specific incident examples. Virginia's mitigation plan documents a 2019 ransomware attack on Smyth County Public Schools, which "*temporarily paralyzed its network across the school system*" and required the restoration of "*significant amounts of data from backups*" (VA, SHMP). These historical references support the inclusion of cyber risk by showing that such incidents have already affected states and local entities.

Future Probability

(16 SHMPs, 2 SEPs). Some plans included assessments of the likelihood of future cyberattacks. These discussions often cited increasing digital dependency and identified specific vulnerabilities. New Jersey's mitigation plan states, "*The sensitive data housed on the computer networks in State buildings are highly vulnerable to this hazard*" (NJ, SHMP). A few plans provided probabilistic estimates. North Carolina's mitigation plan estimates a "*between 1 and 33.3 percent annual probability*" of a severe cyberattack (NC, SHMP), while noting that rapid technological change complicates long-term forecasting. Although some plans conveyed lower expectations of severe incidents based on prior experience, most described increasing risk associated with growing reliance on digital infrastructure.

Cyber Disaster Management Cycle

This category captures how state plans address cybersecurity across the emergency management cycle—mitigation, response, recovery, and preparedness.

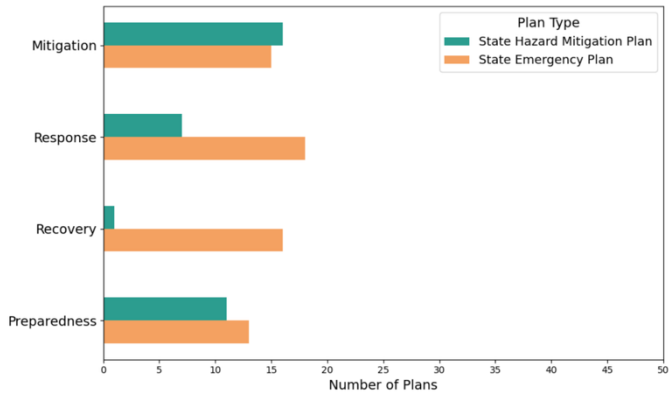

Figure 5. Number of SHMPs and SEPs containing at least one coded text segment in each phase of the Cyber Disaster Management Cycle

Mitigation

(16 SHMPs, 15 SEPs). Mitigation content commonly emphasized hardening and risk reduction activities, such as audits, training, and information sharing. Virginia's mitigation plan identifies priorities such as "*routine audits of IT systems,*" "*continuing education for IT professionals and general staff,*" and "*regular checks of IT/cyber infrastructure*" (VA, SHMP). The level of detail varied across plans, but most outlined steps aimed at improving cybersecurity preparedness and long-term risk reduction.

Response

(7 SHMPs, 18 SEPs). Response content appeared more often in SEPs and focused on coordination structures, assigned responsibilities, and activation of incident response protocols. Connecticut's emergency plan describes

how DAS/BITS[3] activates its "*Cyber Incident Response Plan*" and convenes a "*Centralized Computer Security Incident Response Team (CSIRT)*" to manage incidents (CT, SEP). Some plans also addressed operational requirements. Michigan's emergency plan includes provisions to "*provide IT systems support to state agencies under all circumstances, including crisis or emergency, attack, stabilization, and reestablishment*" (MI, SEP). Across plans, response content tended to be the most operationally oriented phase, although the degree to which plans specified triggers, escalation pathways, and coordination procedures varied.

Recovery

(1 SHMPs, 16 SEPs). Recovery was the least developed subcategory, with many plans offering only high-level intentions rather than operational protocols. Washington's emergency plan provided broad statements for agencies to "*protect (and, if needed, restore) electronic communication systems, information, and services from damage, unauthorized use, and exploitation*" (WA, SEP). A small subset provided more detailed guidance. Alabama's emergency plan, for example, includes recovery-focused questions for response teams, such as "*Where will responders pull recovery and backups from? How will infected systems be deployed back into production? What operations will be restored during the recovery phase?*" (AL, SEP). Recovery detail was relatively limited, even though the excerpts that did appear referred to restoration, backup use, and service restoration priorities.

Preparedness

(11 SHMPs, 13 SEPs). Preparedness content varied widely. Some plans emphasized education and awareness initiatives. North Dakota's mitigation plan notes that "*the Governor has prioritized cybersecurity education to assure improved resilience to cyberattacks*" (ND, SHMP). Other plans focused on planning and exercises. The Mississippi emergency plan spoke of the importance of "*strategic planning and exercises*" to address the challenges posed by multiple or complex cyber incidents (MS, SEP). Some also addressed resource planning. Washington's emergency plan directs agencies to conduct "*resource capabilities and needs assessments for disaster scenarios"* across personnel, equipment, facilities, and cyber systems (WA, SEP). Overall, preparedness content often reflected recognition of the problem, but the degree to which plans specified regular training cycles, exercise programs, or resource commitments differed greatly.

Cyber Policies & Procedures

This category examines how state plans address the governance, operational protocols, and detection and reporting processes necessary for managing cybersecurity incidents. While coverage varied, plans often included content on agency responsibilities, risk management standards, strategic planning, and reporting requirements.

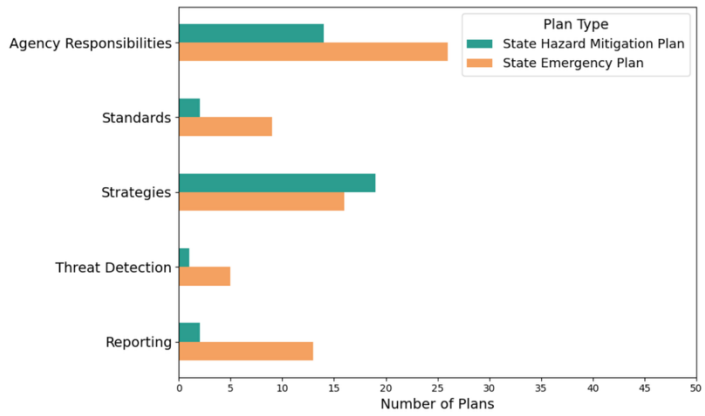

Figure 6. Number of SHMPs and SEPs containing at least one coded text segment in each Cyber Policies & Procedures subcategory

Agency Responsibilities

(14 SHMPs, 26 SEPs). Agency responsibilities were the most consistently represented subcategory within Cyber Policies & Procedures. Plans often identified key organizations involved in cyber response, and clarified the roles assigned to these agencies. For example, North Carolina's emergency plan highlights the role of the Joint Cybersecurity Mission Center (JCMC), which coordinates "*all operational response activities and resource allocations*" and facilitates communication with the State EOC, the Governor's office, and federal partners (NC, SEP). These sections show that some states describe cyber incidents in ways that involve cross-agency coordination rather than isolated technical events.

Standards

(2 SHMPs, 9 SEPs). Only a small subset of plans referenced cybersecurity Standards or guidelines for protecting

[3] Department of Administrative Services/Bureau of Information Technology Solutions (DAS/BITS) – https://ct.gov

state data, systems, and infrastructure. Where present, cybersecurity standards were often framed in terms of data protection and system reliability, though detailed implementation practices were rarely outlined. Nevada's hazard mitigation plan calls for "*risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information*" across state systems (NV, SHMP). Where standards were mentioned, they were often framed at a high level and rarely paired with implementation details or accountability mechanisms.

Strategies

(19 SHMPs, 16 SEPs). Many plans acknowledged the evolving nature of cyber threats and included strategies to enhance resilience. Strategies often referenced national frameworks and highlighted the need for coordinated planning and exercises. South Carolina's emergency plan cites the National Cyber Incident Response Plan and notes that "*the frequency of cyber incidents is increasing*" and that response requires "*deliberate planning, coordination, and exercises to respond effectively*" (SC, SEP). Some plans also described state-led initiatives. Michigan's emergency plan includes efforts to "*improve the state's cybersecurity posture; coordinate cyber information sharing; and proactively manage state cyber risks*" (MI, SEP). Strategy content varied but generally emphasized the importance of proactive and coordinated planning.

Threat Detection

(1 SHMPs, 5 SEPs). Threat Detection was among the least frequently addressed topics. Where included, content focused on enhancing network monitoring and early warning capabilities. Arizona's hazard mitigation plan sets a goal to "*improve and expand the cyber threat/incident alerting and notification capability*" to support timely detection and response (AZ, SHMP). Few plans provided detailed descriptions of detection tools or operational protocols. The limited number of references to Threat Detection indicates that early identification and alerting processes were specified less often than role assignment or general strategy statements.

Reporting

(2 SHMPs, 13 SEPs). Communication and reporting processes were addressed in several plans, with a focus on both immediate notification and post-incident documentation. Wisconsin's emergency plan states: "*Prompt notification of key personnel in a cyber-threat or incident is critical. Each agency… response shall identify key personnel and a means to rapidly alert them*" (WI, SEP). In addition to notification requirements, some plans provided guidance on post-incident reporting to address legal compliance and inform future planning. Reporting content was uneven and ranged from immediate notification procedures to broader post-incident documentation requirements.

DISCUSSION

This study examined how cybersecurity is addressed in U.S. state-level emergency and mitigation planning documents. While most plans referenced cybersecurity, the depth and focus of that coverage varied significantly. SEPs tended to emphasize agency responsibilities and operational response protocols, while SHMPs more often focused on risk identification and general mitigation strategies. This distinction aligns with prior work that differentiates between operational readiness and strategic risk reduction (Habets et al., 2024) and has important implications for cyber crisis governance.

Emerging patterns across both plan types point to increased attention to cyber threats and government responsibilities. This suggests that states increasingly recognize cybersecurity as a planning concern. However, other critical areas—such as recovery planning, detection capabilities, and governance frameworks—remain comparatively underdeveloped. This pattern is consistent with prior critiques of hazard mitigation planning as more aspirational than operationally strategic (Gall et al., 2024). Even when mitigation or preparedness are addressed, plans often provide limited guidance on escalation thresholds, cross-agency reporting, recovery decision points, and procedures that can be exercised in practice. Similar gaps have been identified in hospital emergency planning for cyber incidents (Sullivan et al., 2023).

The uneven treatment of cybersecurity also reflects broader trends observed in cybersecurity policy research. As Ganapati et al. (2023) state, policy development often advances more quickly than implementation or long-term strategic planning. In many of the plans analyzed here, cyber content was not accompanied by cyber-specific annexes or detailed recovery and continuity protocols, pointing to a broader weakness in structural cyber resilience. Groenendaal et al. (2022) argue that organizational preparedness must extend beyond prevention to include adaptive frameworks capable of absorbing and responding to cyber crises, a shift that is largely absent from the state plans analyzed here.

Implications for State Cyber Emergency Planning

Addressing these gaps does not require embedding highly technical playbooks in core emergency planning documents. It does, however, require more explicit guidance on how cyber incidents move through emergency governance structures. More operational cyber planning would specify when an incident remains agency-managed versus when it triggers broader state coordination, how information should move from technical personnel to emergency management leadership and external partners, and how recovery should address restoration priorities, backup validation, continuity dependencies, and interagency resource-sharing. These elements could be incorporated directly into SEPs or SHMPs, or addressed through referenced cyber-specific annexes, without overburdening the main plan.

The need for greater specificity is especially pronounced for detection, reporting, and recovery. Plans often identify responsible agencies, but far fewer explain how incidents are detected, how situational awareness is established, or how notification and escalation should proceed across organizations. This matters because early detection and structured reporting are not just technical functions; they are governance mechanisms that shape whether decision-makers can develop a common operating picture quickly enough to coordinate action. Likewise, the limited treatment of recovery is consequential because cyber incidents often require extended restoration, sequencing decisions about which services are restored first, and coordination across agencies and infrastructure operators. Plans that assign responsibility without specifying these workflows risk leaving a gap between recognizing cyber risk and coordinating action during a crisis.

The distinction between SHMPs and SEPs also points to different opportunities for improvement. For SHMPs, the most useful contribution may be to strengthen expectations for reducing cyber risk over time, including more explicit treatment of continuity dependencies, critical system vulnerabilities, and mitigation priorities tied to essential services. For SEPs, the more immediate need is procedural clarity: who must be notified, under what conditions, through which channels, and how cyber incidents are integrated into broader emergency coordination structures. In both cases, the goal is not to make every plan identical, but to establish clearer coordination logic that can be exercised, adapted, and evaluated during real incidents.

These gaps may also require clearer direction at the state level and stronger alignment with federal frameworks, particularly for how cyber incidents are escalated, coordinated, and documented across jurisdictions. More targeted guidance could help states translate broad all-hazards expectations into cyber-specific planning provisions for detection, reporting, continuity, and recovery, while still preserving flexibility in implementation. Better harmonization across jurisdictions may also reduce fragmentation, especially for incidents involving shared infrastructure, regional service providers, or cross-state emergency coordination.

Broader Relevance and Comparative Implications

Although this study focuses on U.S. state-level plans, the crisis governance challenges it identifies are not unique to the U.S. context. Many jurisdictions rely on multi-level plans and guidance documents to coordinate preparedness, response, and recovery across public agencies and critical infrastructure operators, and cyber incidents routinely cross organizational and geographic boundaries. The patterns we observed—especially the stronger attention to risk framing and role definition than to detection, reporting, recovery, accountability, and learning mechanisms—highlight a set of planning "pressure points" that may generalize to other national and subnational planning systems. More broadly, the coding framework and document-analysis approach used here can be adapted to examine how cyber risks are incorporated into disaster planning in other countries (e.g., national emergency plans, sectoral resilience strategies, and regional civil protection plans), supporting comparative work on cyber crisis governance across jurisdictions.

In sum, the growing presence of cybersecurity in SHMPs and SEPs marks an important step forward, but acknowledgment alone is not enough. Progress will depend on more clearly specifying how cyber incidents are detected, escalated, coordinated, and recovered from within state emergency governance systems.

Limitations & Future Work

This study has several limitations. It focused on publicly available state plans, and non-public operational documents may contain additional cybersecurity content not captured here. While efforts were made to obtain the most current versions of state plans, some documents may not reflect the latest revisions because state websites and update practices vary. In addition, variations in document structure and terminology required interpretive decisions during coding that may have influenced the findings.

Future work could incorporate non-public planning documents where available and include interviews with state emergency management officials to examine how cybersecurity planning is operationalized in practice.

Comparative analysis across different types of states, such as by size or geographic region, may also provide additional insights. Expanding the scope of analysis to include local and regional plans would further contribute to understanding how cybersecurity considerations are integrated across multiple levels of U.S. disaster management. Finally, extending this analysis to comparable planning documents in other countries would support cross-jurisdictional comparison of cyber crisis governance.

CONCLUSION

As cyber threats continue to intersect with traditional disaster risks, integrating cybersecurity into state-level disaster planning remains an important area of focus. This study provides a national-level assessment of how U.S. states address cybersecurity in their hazard mitigation and emergency plans. While many states now acknowledge cyber risks and assign responsibilities, planning content related to detection and reporting mechanisms, recovery and continuity, and enforceable governance standards remains limited.

Strengthening these areas will likely require sustained collaboration between state and federal stakeholders, alongside clearer alignment across jurisdictions. Incorporating more actionable guidance for preparedness, response coordination, recovery, and organizational learning can help move plans beyond acknowledgement toward operationally meaningful cyber crisis governance. Continued attention to cybersecurity in state-level planning can support more effective, coordinated responses to future cyber incidents and cascading disasters.

ACKNOWLEDGMENTS

The authors acknowledge support from the U.S. National Science Foundation under Award No. 2336409.

REFERENCES

Chakraborty, S., Mombeshora, E. M., Clark, K. P., & Mbavarira, T. S. (2024). Understanding of Cyber-Attack Vulnerabilities During Natural Disasters and Discussing a Cyber-Attack Resiliency Framework. *SoutheastCon 2024*, 466–471. https://doi.org/10.1109/SoutheastCon52093.2024.10500233

Frazier, T. G., Walker, M. H., Kumari, A., & Thompson, C. M. (2013). Opportunities and Constraints to Hazard Mitigation Planning. *Applied Geography*, *40*, 52–60. https://doi.org/10.1016/j.apgeog.2013.01.008

Gall, M., Li, P., & Friedland, C. J. (2024). Strategic hazard mitigation planning. *International Journal of Disaster Risk Reduction*, *114*, 104923. https://doi.org/10.1016/j.ijdrr.2024.104923

Ganapati, S., Ortega Franco, L., & Le, A. N. (2023). American State Government Cybersecurity Policies. *Proceedings of the 24th Annual International Conference on Digital Government Research*, 637–638. https://doi.org/10.1145/3598469.3598540

Groenendaal, J., Helsloot, I., & Reuter, C. (2022). Towards More Insight into Cyber Incident Response Decision Making and its Implications for Cyber Crisis Management. *Proceedings of the International ISCRAM Conference*. https://idl.iscram.org/files/jellegroenendaal/2022/2468_JelleGroenendaal_etal2022.pdf

Grossman, T., & Smith, T. (2024). *2023 RTF Global Ransomware Incident Map: Attacks Increase by 73%, Big Game Hunting Appears to Surge*. Institute for Security + Technology. https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map/

Habets, M., Jackson, S. L., Baker, S. L., Huang, Q., Blackwood, L., Kemp, E. M., & Cutter, S. L. (2024). Evaluating the Quality of State Hazard Mitigation Plans Based on Hazard Identification, Risk, and Vulnerability Assessments. *Journal of Homeland Security and Emergency Management*, *21*(3), 331–358. https://doi.org/10.1515/jhsem-2022-0060

Kishi, K., Kosaka, N., Kura, T., Kokogawa, T., & Maeda, Y. (2017). Study on Integrated Risk-Management Support System. *Proceedings of the 14th ISCRAM Conference*, 432–444. https://idl.iscram.org/files/koujikishi/2017/2032_KoujiKishi_etal2017.pdf

Krippendorff, K. (2019). Content Analysis: An Introduction to Its Methodology. SAGE Publications, Inc. https://doi.org/10.4135/9781071878781

Lawson, C. T., & Tobey, A. (2022). The Role of Natural Hazard Mitigation Plans in an Age of Pandemics. *Progress in Disaster Science*, *16*, 100267. https://doi.org/10.1016/j.pdisas.2022.100267

Lee, E. A., Lacalle, D. E., & Painter, W. L. (2025). *FEMA: Increased Demand and Capacity Strains* (In Focus IF12834). Congressional Research Service.

Lee, J. Y.-H., Chou, C.-Y., Chang, H.-L., & Hsu, C. (2024). Building Digital Resilience Against Crises: The Case of Taiwan's COVID-19 Pandemic Management. *Information Systems Journal*, *34*(1), 39–79.

https://doi.org/10.1111/isj.12471

Lindström, N. B., Razmerita, L., Prokopenko, S., & Popovych, N. (2024). Building Digital Resilience in Major Shocks: How Ukrainian Organizations Enact Digital Transformation in Times of War. *Hawaii International Conference on System Sciences 2024 (HICSS-57)*. https://aisel.aisnet.org/hicss-57/os/global_crises/4

Lyles, W., Berke, P., & Smith, G. (2014). A Comparison of Local Hazard Mitigation Plan Quality in Six States, USA. *Landscape and Urban Planning*, *122*, 89–99. https://doi.org/10.1016/j.landurbplan.2013.11.010

Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment*, *11*(4), 507–518. https://doi.org/10.1108/IJDRBE-07-2019-0046

Radianti, J. (2025). Navigating Digital Resilience in Complex Emergency Management Environments. *Proceedings of the International ISCRAM Conference*. https://doi.org/10.59297/tz4wre14

Schreier, M. (2012). Qualitative Content Analysis in Practice. SAGE Publications Ltd. https://doi.org/10.4135/9781529682571

Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. (2023). A National Survey of Hospital Cyber Attack Emergency Operation Preparedness. *Disaster Medicine and Public Health Preparedness*, *17*, e363. https://doi.org/10.1017/dmp.2022.283