International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Ransomware Resilience for Municipal Infrastructure

Venkata Kartheek Reddy Somasani

Executive Summary

Municipal and local-government networks have become attractive ransomware targets because they combine broad public exposure, heterogeneous legacy estates, high service-criticality, and limited tolerance for downtime. The FBI's 2024 Internet Crime Report states that ransomware remained the most pervasive cyber threat to U.S. critical infrastructure, while CISA's updated #StopRansomware guidance emphasizes that modern events typically involve both encryption and data extortion rather than simple file locking alone. [1], [2].

Public reporting on a large U.S. municipality's 2023 ransomware event illustrates the operational consequences: weeks of restoration activity, extensive service disruption, prolonged recovery engineering, data-exposure notifications, and a multimillion-dollar remediation program. Official reporting further indicates that the attackers initially used a compromised service account, moved internally with legitimate remote-management tooling, and prepared command-and-control beacons before launching encryption at scale. [4], [5], [6].

This paper develops a vendor-neutral IEEE-style blueprint for municipal ransomware resilience. It treats local government as an enterprise environment containing multiple high-impact enclaves—general municipal services, public safety, justice, finance/ERP, and HR/PII—and proposes a layered architecture built on trust zones, segmentation, strong identity, telemetry, and immutable recovery. The paper aligns the architecture and playbook with CISA, NIST, IC3, and state/local guidance, while retaining NIST SP 800-82 only as a supporting reference for mixed-environment governance rather than as an OT design basis. [2], [3], [8], [9], [10], [18], [21].

The central thesis is straightforward: municipal ransomware resilience is not a product acquisition problem but an architectural discipline. Municipalities that reduce trust, constrain east–west movement, protect administrative paths, centralize high-fidelity telemetry, and rehearse restoration against immutable backups can materially reduce blast radius and restore priority services faster and with greater confidence. [2], [3], [8], [10], [12], [13], [14].

Abstract: Ransomware remains a continuity threat for municipal infrastructure because it targets the availability of public services as directly as it targets data confidentiality. This paper presents a vendor-neutral reference architecture and operational playbook for municipal/local-government networks, synthesizing public-sector incident lessons and authoritative guidance from CISA, NIST, IC3, and state-level cyber programs. The proposed architecture integrates next-generation firewalls, IDS/IPS, URL and DNS filtering, SD-WAN policy segmentation, SIEM/SOAR, EDR/EPP, packet analysis, IAM/MFA, RADIUS-backed AAA, 802.1X network access control, protected privileged-access workflows, secure remote access using IPsec/IKEv2, and immutable/offline backup vaults. The architecture is organized around segmented trust zones—External/Cloud, DMZ, Control Zone, management/monitoring enclaves, and a generic protected boundary for isolated sensitive services—to reduce lateral movement and preserve recovery trust. A lifecycle playbook mapped to NIST SP 800-61 emphasizes preparation, detection and analysis, containment, eradication and recovery, and post-incident improvement. Measurable outcomes include reduced dwell time, faster isolation, improved restore confidence, and shorter restoration intervals for priority municipal services. The result is a repeatable, cloud-agnostic resilience model for local governments seeking to prevent, contain, and recover from ransomware while sustaining public trust and continuity of operations. [2], [3], [8], [9], [10].

Keywords: *ransomware resilience, municipal cybersecurity, local government networks, defense in depth, zero trust, incident response, IAM, MFA, RADIUS, DNS filtering, SIEM/SOAR, EDR, immutable backup, NAC, public safety, finance/ERP.*

Disclaimer: This paper uses anonymized, vendor-neutral descriptions and publicly available sources; identifying operational details are intentionally generalized. It is provided for defensive and educational purposes only. Changes to production systems should occur only under formal authorization, change control, and legal review.

[1]*City of Dallas, USA*

Introduction

Municipal networks differ from many commercial environments because they are simultaneously broad, public-facing, and mission-bearing. A single municipal estate can contain citizen portals, finance and payroll systems, justice and records functions, public safety interfaces, directory infrastructure, endpoint fleets, remote sites, contractor access paths, and third-party integrations. As CISA's localities toolkit observes, communities depend on local governments to maintain trusted digital services, while the toolkit itself was designed to help officials make near-term and enduring progress against escalating cyber risk. [7].

Ransomware is especially damaging in this setting because its effects extend beyond data unavailability. In municipal environments, ransomware interrupts payments, permitting, public records access, court workflows, administrative communications, and emergency support services. The IC3 annual report and CISA's #StopRansomware guidance both frame ransomware as a persistent operational threat whose consequences include service interruption, data theft, extortion pressure, and prolonged restoration efforts. [1], [2].

A widely reported 2023 incident involving a large U.S. municipality is valuable not because it is unique, but because it is typical of the modern municipal problem set. Official reporting described a month-long intrusion window before encryption, use of a basic service account for initial access, lateral movement with legitimate remote-management tools, deployment of command-and-control beacons, data exfiltration, and a recovery program that required large-scale remediation spending and prolonged restoration. [4], [5].

Accordingly, this paper argues that ransomware resilience for municipal infrastructure should be written as an architectural and operational discipline rather than as a checklist of products. It focuses on the municipal enterprise network: how to contain trust, defend identity, isolate services, secure remote access, preserve logs and evidence, and restore business-critical systems in a measured order without reintroducing compromise. [2], [8], [10].

Threat Landscape and Problem Framing

Cyber Breach

The primary threat category for this paper is cyber breach: unauthorized access, ransomware deployment, data exfiltration, credential theft, abuse of trusted tools, and lateral movement across municipal services. The FBI's 2024 reporting states that ransomware remained the most pervasive threat to critical infrastructure, while CISA's guide emphasizes that defenders should plan for both data extortion and operational disruption. [1], [2].

The municipal case literature shows why these events are so difficult to contain once trust is lost. In the 2023 large-city case, the attackers reportedly used a compromised service account, moved internally with legitimate third-party remote-management utilities, and prepared their environment before the disruptive phase was detected. That sequence reinforces a key design lesson for local governments: the decisive controls are those that reduce identity abuse, constrain east–west movement, and separate administrative pathways from ordinary user pathways before encryption begins. [4], [5].

Insider Threat Breach

A second category is insider threat breach, which includes malicious misuse of authorized access and negligent actions such as credential reuse, unsafe approval of remote access, poor handling of sensitive data, or accidental activation of malicious content. In municipal environments, insider risk is amplified by distributed departments, rotating contractors, seasonal staff, emergency exceptions, and shared administrative practices. NIST's incident-response guidance and CISA's ransomware guidance both assume that compromised credentials and overbroad privileges materially worsen real incidents. [2], [8], [10].

The local-government implication is that insider risk cannot be handled solely through awareness training. It must be engineered into the architecture through least privilege, persistent MFA, port-based access control, privileged access workstations, session recording, short-lived elevation, and sharply bounded jump paths. Identity is not merely an access-control concern; it is the municipality's primary containment boundary once endpoint compromise begins. [10], [13], [15].

Chemical and Biological Breach as an Adjacent Municipal Consequence Category

A strictly enterprise-focused municipal ransomware paper does not treat chemical or biological breach as a primary cyber category. However, it remains relevant as an adjacent consequence category because local governments support hazardous-materials response, public-health coordination, emergency notification, and continuity-of-operations planning during contamination or disease events. Federal and public-health sources note that local governments and local health departments have defined preparedness and response roles for hazardous materials incidents and broader public-health emergencies. [19], [20].

For this reason, chemical/biological breach is retained here only in a narrow sense: ransomware may not directly create such incidents in the enterprise network, but it can degrade the municipal communications, dispatch, records, coordination, and reporting systems needed to manage them. That makes cyber resilience part of municipal emergency-management resilience, especially for public safety and continuity officials. [19], [20].

Standards, Guidance, and Method

This paper is grounded in primary U.S. guidance rather than vendor playbooks. CISA's #StopRansomware Guide provides the baseline prevention and response practices; NIST IR 8374Rev.1 frames ransomware risk management in CSF-aligned terms; NIST SP 800-61 Rev. 3 updates incident-response recommendations and integrates them with cyber risk management; CISA's federal playbooks supply operationally useful response structure; and NIST SP 800-207 provides the zero-trust rationale for resource-centric and policy-centric access decisions. [2], [3], [8], [9], [10].

Additional supporting guidance comes from CISA's Known Exploited Vulnerabilities catalog, the CISA Cybersecurity Performance Goals, NIST log-management and forensic guidance, IC3 reporting guidance, and state-level incident reporting resources. These sources matter because municipal ransomware resilience is not only about prevention; it is also about telemetry quality, legal reporting, evidentiary preservation, restoration planning, and prioritization under constrained staff and budget. [11], [12], [13], [14], [18], [23].

NIST SP 800-82 and ISA/IEC 62443 are retained only as supporting references. They remind municipal architects that some local governments operate mixed environments or safety-sensitive systems, and that segmentation discipline and security-zone thinking remain useful beyond classical enterprise networks. This paper, however, does not treat OT, SCADA, or water-system design as normative scope. [21], [22].

Methodologically, the paper combines four inputs: authoritative federal and state guidance, public reporting on a large municipal ransomware incident, user-supplied architectural diagrams and mapping tables, and a synthesis of resilient municipal design patterns into a single vendor-neutral reference architecture. The resulting model is intentionally platform-agnostic and suitable for adaptation to hybrid, fully on-premises, or mixed cloud environments. [2], [7], [9], [18].

Vendor-Neutral Reference Architecture and Design Patterns

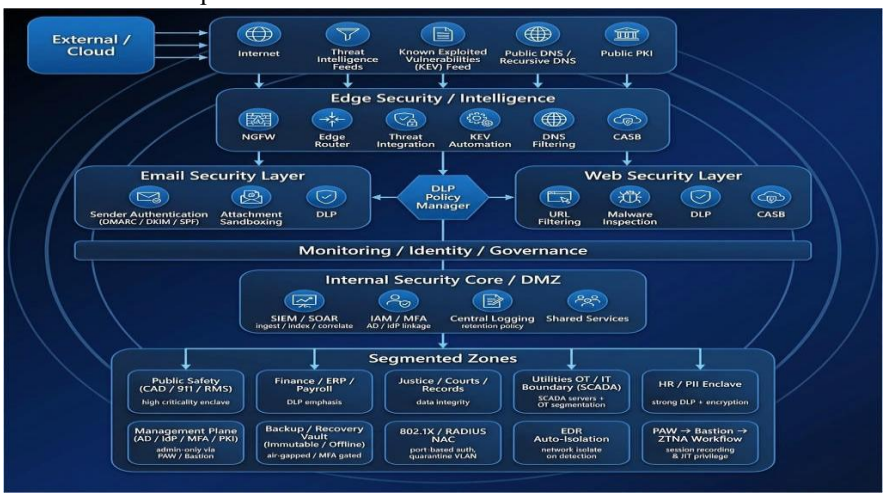


Figure 1. Municipal ransomware resilience architecture.

Architectural Logic

The architecture is organized around five trust layers: External/Cloud, Edge Security and Intelligence, DMZ, Control Zone, and a generic Protected Boundary for isolated or especially sensitive services. The purpose is not visual neatness but blast-radius reduction. CISA and NIST repeatedly emphasize segmentation, privileged-access control, logging, backup protection, and rapid response as the controls most likely to limit ransomware spread and accelerate recovery. [2], [3], [8], [10], [13].

The **External/Cloud** layer includes Internet exposure, threat-intelligence and KEV feeds, public DNS/PKI, and cloud-agnostic private connectivity. The speculative value of threat feeds is limited unless they drive action, so the architecture assumes KEV-driven prioritization, DNS-based blocking, and dynamic policy updates for exposed services. CISA explicitly recommends using the KEV catalog as an input to remediation prioritization because it reflects vulnerabilities known to be exploited in the wild. [11].

The **Edge Security and Intelligence** layer consolidates email security, secure web gateway functions, DNS filtering, NGFW policy enforcement, IDS/IPS, and threat integration. This layer is where municipalities should reduce initial-access probability through sender authentication, sandboxing, URL/content filtering, geo-blocking where justified, malicious-domain blocking, and inspection of high-risk traffic flows. CISA's ransomware guidance and performance goals both stress MFA, filtering, vulnerability management, and protective controls that demonstrably reduce common intrusion paths. [2], [12].

The **DMZ** is split logically between a public-services DMZ and an administrative DMZ. The public-services DMZ hosts reverse proxies, API gateways, and citizen-facing access points. The administrative DMZ is more restrictive: it is the only approved transit path for privileged operations and is anchored on PAWs, bastions, MFA, session recording, and policy-enforced ZTNA or tightly bounded VPN access. This reflects NIST SP 800-207's shift away from implicit network trust toward continuous, resource-scoped authorization. [10].

The **Control Zone** contains segmented municipal enclaves rather than one "inside network." At minimum, municipalities should isolate general municipal services, public safety, justice/records, finance/ERP, and HR/PII. The control objective is not simply compliance separation; it is to avoid single-event trust collapse. In the reported municipal case, recovery complexity was worsened by the need to rebuild services methodically after a broad compromise that affected many functions. [4], [5], [6].

The **Protected Boundary** is a generic label that replaces OT-specific phrasing while preserving the architectural idea of an isolated zone for sensitive or non-routable services. In different municipalities this may represent specialized justice, emergency communications, regulated data, or high-risk third-party interfaces. The paper labels it generically because the trust principle matters more than the sector label. [10], [21].

Core Design Patterns

The reference architecture uses recurring design patterns rather than vendor products.

Pattern	Primary purpose	Control logic	Example measurable outcome
NGFW + IDS/IPS	Reduce initial access and enforce north–south policy	Inline filtering, threat signatures, geofencing, TLS inspection where lawful	Reduced internet-exposed attack surface; fewer preventable ingress events
URL/DNS filtering	Block malicious destinations early	Domain reputation, recursive DNS sink holing, SWG policy	Lower C2 success rate; earlier detection of staging behavior
SD-WAN policy segmentation	Preserve segmentation across distributed sites	Route by policy, keep sensitive flows on inspected paths, isolate affected sites quickly	Faster site quarantine without collapsing whole WAN
IAM/MFA/RADIUS + 802.1X NAC	Contain identity misuse and unauthorized edge access	Strong auth, device-aware access, quarantine VLANs, centralized AAA	Reduced lateral movement through stolen credentials or rogue devices
PAW → Bastion → ZTNA / IPsec	Protect administrative actions during both normal operations and recovery	Dedicated admin endpoints, MFA-only jump paths, just-in-time privilege	Safer restoration and lower probability of admin-path reuse by attackers
SIEM/SOAR + packet analysis + EDR/EPP	Correlate, detect, and scope incidents	Central log ingestion, alerting, hunting, endpoint isolation, network evidence	Faster dwell-time reduction and higher-confidence containment
Immutable/offline backup vault	Preserve restoration trust	MFA-gated destructive actions, offline or logically isolated copies, restore testing	Higher restore confidence and lower probability of backup sabotage

The table above maps cleanly to federal guidance. CISA's guide emphasizes MFA, filtering, segmentation, incident preparation, evidence retention, and backup protection; NIST IR 8374Rev.1 and SP 800-61r3 elevate preplanned response and tested recovery as core ransomware risk-management outcomes rather than optional mature-state capabilities. [2], [3], [8].

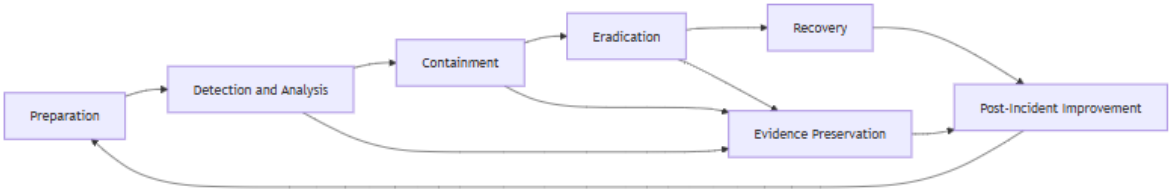
Tailored Recommendations by Municipal System Type

Municipal system type	Highest risks	Priority architectural choices	Operational priority
General municipal services	Broad exposure, commodity phishing, third-party web dependencies	SWG, email security, DMZ reverse proxy, DNS filtering, EDR, MFA	Restore portals and collaboration without reintroducing trust to compromised assets
Public safety	Service continuity, emergency communications, dispatch dependency, strict change control	Strong enclave separation, admin-only jump paths, redundant communications, restricted vendor access, aggressive logging	Maintain dispatch-supporting services and emergency coordination even under degraded IT conditions
Finance / ERP / Payroll	Data exfiltration, payment fraud, business-email compromise, PII exposure	DLP, tighter egress control, payment network isolation, immutable records backup, privileged approval workflows	Restore payment and payroll integrity before reconnecting broad integrations

The public-safety row deserves particular emphasis. CISA's public-safety cybersecurity materials warn that ransomware can affect emergency response operations and emergency communications resources. Consequently, public-safety-related systems should have stricter enclave boundaries, fewer standing administrative accounts, and

alternate continuity paths than ordinary administrative applications. [19].

Incident-Response Lifecycle Flow



This lifecycle follows the logic of NIST incident-response guidance and is deliberately recursive rather than linear. Lessons learned, control gaps, and restoration findings should feed directly back into preparation baselines, tabletop exercises, segmentation maps, and privileged-access governance. [8], [9], [14].

Ransomware Resilience Playbook and Measures of Success

Playbook Mapped to NIST SP 800-61

Preparation. Municipal preparation begins with authoritative asset inventory, service-tier classification, administrative-path mapping, credential hygiene, tested backups, and exercised communications. NIST IR 8374Rev.1 explicitly states that ransomware response and recovery plans should be tested periodically so that assumptions remain current; CISA's guidance similarly treats playbook preparation, offline backups, MFA, and segmentation as essential. [2], [3], [8].

Detection and analysis. Municipalities should correlate perimeter, DNS, identity, endpoint, and network telemetry into a single investigative workflow. NIST's log-management and forensic guidance remains directly relevant here: logs are necessary for enterprise-wide visibility, and forensic processes should be integrated into incident response rather than bolted on after the fact. [13], [14].

Containment. Containment should prioritize identity and segmentation before mass rebuilding. Disable or rotate compromised credentials, invalidate sessions, quarantine affected VLANs or hosts using NAC and EDR automation, and harden permit lists between enclaves. CISA's playbooks and ransomware guidance support rapid containment actions that favor trust restoration over broad reinstatement of network reachability. [2], [9], [12].

Eradication and recovery. Rebuild from known-good images or gold baselines, not from partially trusted systems. Restore identity services, logging, backup access, and administrative control paths before reconnecting major applications. Protect recovery operations with MFA, session recording, and immutable/offline backups. Reported municipal incident lessons show that recovery can be prolonged and costly when legacy systems, unsupported software, and technical debt complicate restoration. [4], [5], [6].

Post-incident improvement. After-action review should be mandatory. Update segmentation policies, recovery runbooks, remote-access configurations, incident thresholds, vendor-access requirements, and cyber insurance evidence packages. State-level redbook guidance and NIST both emphasize lessons learned and planning improvements after a major incident. [8], [18].

Measurable Success Criteria

A municipal ransomware program should define success in operational terms rather than procurement terms.

Metric	Suggested target direction	Why it matters
Mean time to credential completion	Down	Identity misuse is often the decisive spread vector
Mean time to host or VLAN isolation	Down	Faster isolation reduces encryption blast radius

Metric	Suggested target direction	Why it matters
Percentage of critical services with tested restore procedure	Up	Recovery confidence matters more than backup existence alone
Percentage of privileged actions performed through PAW/Bastion paths	Up	Reduces unsafe restoration and admin-path compromise
Percentage of internet-facing assets tracked against KEV	Up	Converts vulnerability knowledge into action
Percentage of endpoints covered by EDR with automatic isolation enabled	Up	Increases containment speed
Percentage of priority services with alternate continuity process	Up	Critical for public safety, courts, and payroll
Time to produce executive incident dashboard and legal-notification package	Down	Supports leadership, reporting, and public trust

These criteria reflect the structure of CISA's performance goals and NIST's ransomware-risk guidance, both of which stress measurable, high-impact practices rather than aspirational maturity language. [3], [12].

Reporting, Legal Coordination, and External Engagement

Ransomware response in local government also requires disciplined external coordination. IC3 explicitly instructs victims to report ransomware incidents and notes that the FBI does not support ransom payment as a response strategy. State-level obligations may also apply quickly; for example, Texas requires certain state and local government entities experiencing security incidents involving regulated data to report within 48 hours of discovery. [18], [23].

Supporting but Non-Normative Cross-Sector References

Although this paper excludes detailed OT and water-system content, the segmentation and zone-thinking discipline found in NIST SP 800-82, ISA/IEC 62443, Claroty's IT/OT discussion, Dragos' ransomware analyses, and WaterISAC's resilience messaging remains conceptually useful as supporting context for municipalities that operate mixed estates or regulated, isolated services. In this paper, however, those materials are retained only as secondary references rather than design authorities. [21], [22], [24], [25], [26-30].

References

[1] FBI Internet Crime Complaint Center, "2024 IC3 Annual Report," 2024. [Online]. Available: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[2] CISA and the Joint Ransomware Task Force, "#StopRansomware Guide," Mar. 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf

[3] Murugiah Souppaya et al., "NIST IR 8374 Rev. 1 (Initial Public Draft), Ransomware Risk Management," Jan. 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8374r1.ipd.pdf

[4] Local-government official report, "THE CITY OF DALLAS RANSOMWARE INCIDENT: MAY 2023

Incident Remediation Efforts and Resolution," Sept. 2023. [Online]. Available: https://dallascityhall.com/DCH%20Documents/dallas-ransomware-incident-may-2023-incident-remediation-efforts-and-resolution.pdf

[5] A. Waldman, "Dallas doles out $8.5M to remediate May ransomware attack," *TechTarget SearchSecurity*, 2023. [Online]. Available: https://www.techtarget.com/searchsecurity/news/366553259/Dallas-doles-out-85M-to-remediate-May-ransomware-attack

[6] Kevin Reece, "Dallas, Texas ransomware attack: The latest recovery efforts," WFAA, 2023. [Online]. Available: https://www.wfaa.com/article/news/local/dallas-ransomware-progress-recovery/287-8fecc192-e4b2-40ce-8f6f-3078d1fac1b4

[7] CISA, "Partnering to Safeguard Localities from Cybersecurity Threats Toolkit," 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-01/23-0070_mayorscybersecuritytoolkit_508c.pdf

[8] Alex Nelson et al., "SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cyber Risk Management," NIST, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[9] CISA, "Federal Government Cybersecurity Incident and Vulnerability Response Playbooks," 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-02/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[10] Scott Rose, "SP 800-207, Zero Trust Architecture," NIST, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[11] CISA, "Known Exploited Vulnerabilities Catalog." [Online]. Available: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[12] CISA, "Cybersecurity Performance Goals 2.0," 2025. [Online]. Available: https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0

[13] Karen Kent, Murugiah Souppaya, "SP 800-92, Guide to Computer Security Log Management," NIST, 2006. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

[14] Karen Kent et al., "SP 800-86, Guide to Integrating Forensic Techniques into Incident Response," NIST, 2006. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

[15] IEEE 802.1 Working Group, "802.1X: Port-Based Network Access Control." [Online]. Available: https://1.ieee802.org/security/802-1x/

[16] S. Kent and K. Seo, "RFC 4301: Security Architecture for the Internet Protocol," IETF, 2005. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4301.html

[17] C. Kaufman *et al*., "RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)," IETF, Oct. 2014. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7296

[18] Texas Department of Information Resources, "Cybersecurity Incident Management and Reporting," and "SB 271 Security Incident," 2024–2025. [Online]. Available: https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting

[19] CISA, "Public Safety Cybersecurity," and "Public Safety Emergency Communications Resources." [Online]. Available: https://www.cisa.gov/public-safety-cybersecurity

[20] FEMA, "Hazardous Response Capabilities," and NCBI, "State and Local Governments — Crisis Standards of Care." [Online]. Available: https://www.fema.gov/emergency-managers/risk-management/hazardous-response-capabilities ; https://www.ncbi.nlm.nih.gov/books/NBK201073/

[21] Keith Stouffer et al., "SP 800-82 Rev. 3, Guide to Operational Technology Security," NIST, 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

[22] ISA, "ISA/IEC 62443 Series of Standards." [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[23] FBI Internet Crime Complaint Center, "Ransomware." [Online]. Available: https://www.ic3.gov/CrimeInfo/Ransomware

[24] Claroty, "IT vs OT Security: Key Differences in Cybersecurity," 2026. [Online]. Available: https://claroty.com/blog/it-and-ot-cybersecurity-key-differences

[25] Dragos, "Dragos Industrial Ransomware Analysis: Q2 2025," 2025. [Online]. Available: https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2025

[26] Alec Davison, "Ransomware Resilience: Renew Your Ransomware Defense with CISA's Updated Guidance," WaterISAC, 2023. [Online]. Available: https://www.waterisac.org/ransomware-resilience-renew-your-ransomware-defense-cisas-updated-guidance

[27] Dr. Brian Gardner, "After Action Review Report of May 3rd Ransomware Incident," Local Government Official Memorandum, 2023. [Online]. Available: https://dallascityhall.com/government/ci

tymanager/Documents/Council%20Materials/After%20Action%20Review%20Report%20%28AAR%29%20of%20May%203rd%20Ransomware%20Incident.pdf

[28] Local-government update, "Update on Ransomware Incident & Personal Data Protection," 2023. [Online]. Available: https://www.dallascitynews.net/update-on-ransomware-incident-personal-data-protection

[29] Candace Sweat and Ken Kalthoff, "Dallas Ransomware Attack Contained, But Ongoing; Police, Fire Service Uninterrupted," 2023. [Online]. Available: https://www.nbcdfw.com/news/local/the-city-of-dallas-says-its-battling-a-ransomware-attack/3250013/

[30] CISA, "State, Local, Tribal, and Territorial Government." [Online]. Available: https://www.cisa.gov/audiences/state-local-tribal-and-territorial-government