INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

EXECUTIVE REPORT

CYBERSECURITY TRAINING EFFECTIVENESS IN TEXAS RURAL HOSPITALS FOR TEXAS HOSPITAL ASSOCIATION

J. CHIALASTRI

Executive Report: Cybersecurity Training Effectiveness in Texas Rural Hospitals for Texas Hospital Association

Introduction

Cybersecurity threats continue to escalate across the healthcare sector, placing rural hospitals in Texas at particularly high risk. These hospitals, the cornerstone of care for their communities, face growing operational and financial strain from a surge in ransomware, phishing, and data breach incidents.[1] [2] [3] Recent high-profile attacks have resulted in prolonged system downtimes, disrupted patient care, and, critically, increased risk to patient safety and data privacy. Small, resource-constrained rural hospitals are disproportionately targeted due to their limited budgets, reliance on aging technology, and chronic shortages of specialized cybersecurity staff. In response to these challenges, Texas requires annual cybersecurity training for all hospital staff in accordance with the Department of Information Resources (DIR) guidelines. [4] [5]

This report synthesizes these alongside academic literature and national best practices to evaluate the effectiveness and limitations of current cybersecurity training, with a specific focus on frequency, delivery methods, tenure-based disparities, departmental involvement, review cycles, perceived policy effectiveness, and feedback mechanisms. It concludes with actionable recommendations targeted to the unique needs of rural Texas hospitals.

Training Frequency: Are Annual Sessions Enough?

- Of participants who answered the question (n=47), 68% of Texas rural hospital staff receive cybersecurity training annually; 21% participate monthly, and 9% report that they have no current training.
- Current Texas Department of Information Resources (DIR) requirements mandate annual training, but do not prescribe refresher frequency or modality. [6]

[1] HIPAA Journal, "Microsoft Cybersecurity Rural Hospital Program 2025 Update," *HIPAA Journal*, 2025, https://www.hipaajournal.com/microsoft-cybersecurity-rural-hospital-program-2025-update/.
[2] Texas Recap, "Massive Cyberattack Hits Texas Hospital Network, Patient Data Compromised," *Texas Recap*, 2025, https://texasrecap.com/massive-cyberattack-hits-texas-hospital-network-patient-data-compromised/.
[3] Chief Healthcare Executive, "Ransomware Attacks Threaten Rural Hospitals: HIMSS 2025," *Chief Healthcare Executive*, 2025, https://www.chiefhealthcareexecutive.com/view/ransomware-attacks-threaten-rural-hospitals-himss-2025.
[4] National Rural Health Association, *Cybersecurity and Rural Health Policy Brief*, 2024, https://www.ruralhealth.us/getmedia/ad0774a2-49b4-4f9a-b2c5-2edf0eaf6bcf/2024-NRHA-Cybersecurity-Rural-Health-policy-brief.pdf.
[5] Rural Health Information Hub, *Cybersecurity Toolkit for Rural Hospitals and Clinics*, 2024, https://www.ruralcenter.org/sites/default/files/Cybersecurity%20Toolkit%20for%20Rural%20Hospitals%20and%20Clinics.pdf.
[6] Texas Department of Information Resources, *Statewide Cybersecurity Awareness Training*, Texas DIR, 2025, https://dir.texas.gov/information-security/statewide-cybersecurity-awareness-training.

- 71% of participants in the Texas Hospital Association Exercise reported significantly improved understanding of threat. Most (76%) had concrete plans to review cybersecurity policies, which suggests that annual online training alone may not drive sustained change.

Academic and Practice Context

Research on adult learning and cognitive retention consistently demonstrates that annual training is insufficient to sustain security-relevant knowledge and vigilance. Studies show that, post-training, phishing and breach awareness decline significantly within 4–5 months.[7] [8] A randomized study of healthcare employees found no statistically significant reduction in phishing susceptibility based on the timing of annual training completion. [7] Conversely, evidence from organizations implementing more frequent, scenario-driven training, including quarterly phishing simulations, shows a notable decline in employee mistake rates and improved breach response times.[9]

Recommendation

- Shift from annual-only to at least semi-annual training, supplemented by quarterly phishing simulations and short, targeted refreshers focused on current attack trends.
- Adopt adaptive "just-in-time" training following incidents or observed vulnerabilities (e.g., failed phishing simulation responses).
- Leverage funding and technical assistance through state and federal grant programs, and partnerships such as Microsoft's Cybersecurity for Rural Hospitals initiative, which includes free ongoing training resources.

[7] Grant Ho, Adriana Mirian, et al. *Phishing Training Effectiveness: Evidence from Oakland 2025* (University of Chicago, 2025), accessed December 10, 2025. https://people.cs.uchicago.edu/~grantho/papers/oakland2025_phishing-training.pdf.

[8] Cookey, I. B., C. M. Ajoku, and P. B. Ogini. "Security Awareness and Phishing Training in Nigerian Institutions." *International Journal of Scientific Research in Education* 18, no. 2 (2025). Accessed December 10, 2025. https://ijsre.com.ng/assets/vol.%2c-18%282%29-cookey%2c-i.-b.%2c-ajoku%2c-c.-m.%2c---ogini%2c-p.-b.pdf

[9] KnowBe4, *"KnowBe4 Research Confirms Effective Security Awareness Training Significantly Reduces Data Breaches,"* press release, accessed December 10, 2025, https:l.//www.knowbe4.com/press/knowbe4-research-confirms-effective-security-awareness-training-significantly-reduces-data-breaches.

Training Delivery and Coverage: Blended Methods and Broad Content

- Online modules are the most common delivery method for cybersecurity delivery, with 94% of respondents.
- The high percentage of participants (71%) who reported significantly improved understanding of threats and 76% who became "very aware" of cyber impacts on patient care underscores the value of interactive, scenario-based formats like tabletop exercises.
- Covered topics include phishing, multi-factor authentication (MFA), HIPAA, incident response, and physical security.

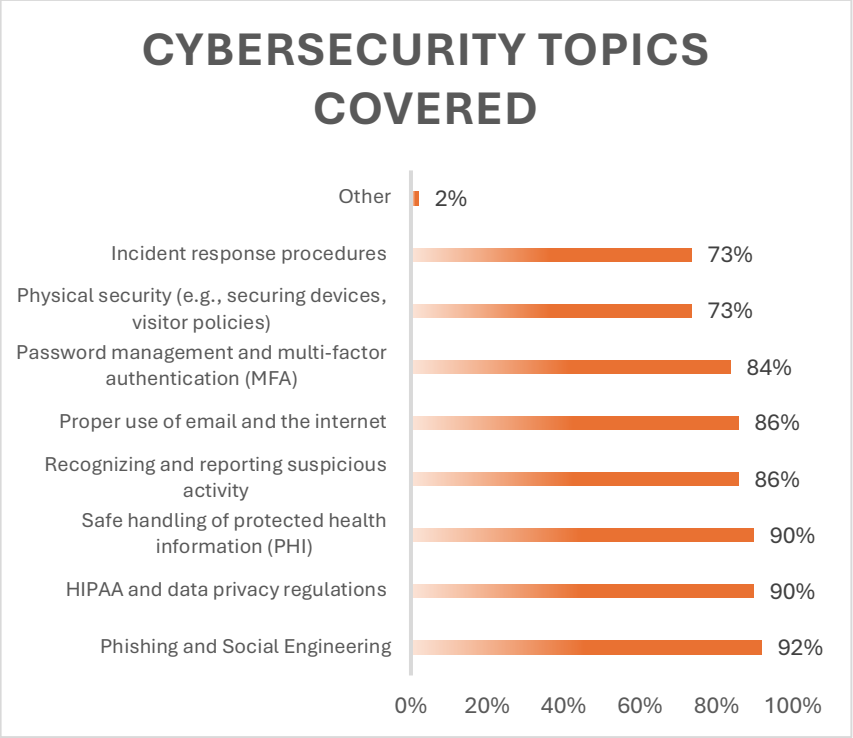

Figure 1 Topics Covered in Cybersecurity Training (n=47)

Academic and Regulatory Alignment

Best-in-class security training programs are rarely monolithic. Blended approaches, which combine in-person events, self-paced online content, interactive phishing simulations, and clear written policy, typically achieve higher training completion rates and retention.[10] [11] For healthcare entities, aligning content with HIPAA Security Rule requirements is not only recommended but necessary for compliance.[12] Interactive, context-specific sessions (e.g., live analysis of real

[10] Jacobs, Jody L., Julie M. Haney, and Susanne M. Furman. *Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study*. Gaithersburg, MD: National Institute of Standards and Technology, 2021. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934952.

[11] Jayatilaka, Asangi, Nathan Beu, Irina Baetu, Mansooreh Zahedi, M. Ali Babar, Laura Hartley, and Winston Lewinsmith. "Evaluation of Security Training and Awareness Programs: Review of Current Practices and Guidelines." *arXiv preprint* arXiv:2112.06356 (2021). https://arxiv.org/pdf/2112.06356.

[12] U.S. Department of Health & Human Services. "HIPAA Training and Resources." *HHS.gov*, 2025. https://www.hhs.gov/hipaa/for-professionals/training/index.html.

phishing attempts or department-specific breach tabletop exercises) outperform generic, static learning modules for knowledge retention and behavioral change.[13] [14]

Content breadth must address evolving attack vectors. Leading resources like HHS "405(d) Knowledge on Demand" and the National Institute of Standards and Technology (NIST) highlight the need for scenario-based learning on phishing, MFA, device security, data handling, incident response, HIPAA privacy, and insider threat awareness.

Departments Involved in Incident Response Planning (%)

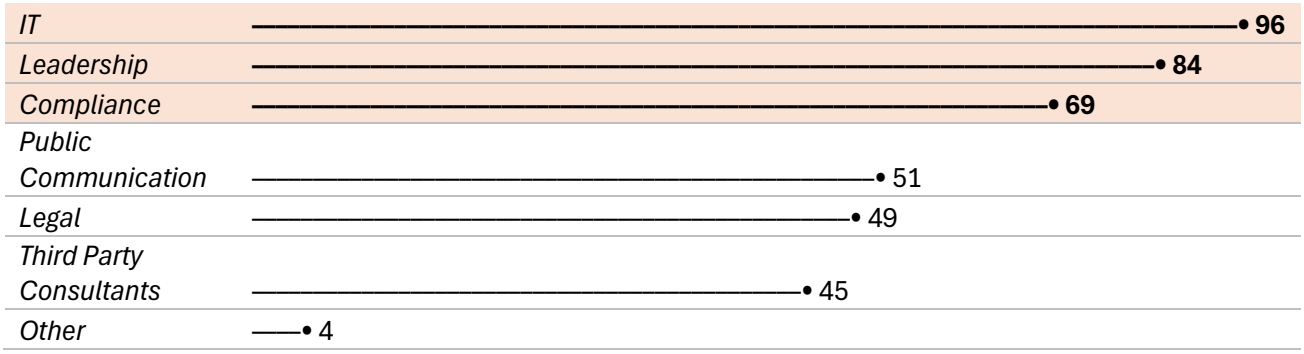

Figure 2 Departments Included in Planning Responses (n=48)

Recommendation

- Explore implementing a blended, multimodal delivery strategy combining scenario-based phishing simulations, routine online modules, and regular dissemination of concise written best practice reminders. [15] [16]
- Ensure content covers all five major threat domains: phishing/social engineering, password/MFA security, HIPAA/data privacy best practices, device security (including medical devices), and response to ransomware or breach incidents.
- Utilize free or subsidized content and simulation platforms (e.g., Microsoft, Google, national nonprofits).

[13] Lin Liu et al., *Understanding the Efficacy of Phishing Training in Practice* (University of Chicago & UC San Diego, 2025), https://people.cs.uchicago.edu/~grantho/papers/oakland2025_phishing-training.pdf.
[14] GTIA North America Cybersecurity Interest Group. *Tabletop Exercises to Build Customer Resilience and Preparedness*. GTIA, 2025. https://gtia.org/hubfs/GTIA%20Cybersecurity%20Guidebook%20for%20ITSPs%20-%20Tabletop%20Exercises.pdf.
[15] A. Reeves, P. Delfabbro, and D. Calic, *"Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue," SAGE Open* 11, no. 2 (2021), https://journals.sagepub.com/doi/pdf/10.1177/21582440211000049.
[16] Fulvio Frati, Georgiana Darau, Nikos Salamanos, and Pantelitsa Leonidou, *"Cybersecurity Training and Healthcare: The AERAS Approach," International Journal of Information Security* 23, no. 2 (January 2024): 1–13, https://doi.org/10.1007/s10207-023-00802-y.

- Plan annual department-specific workshops to bridge hospital roles and address communication breakdowns.

Departmental Involvement: Collaborative Incident Response Improves Outcomes

- High departmental engagement in incident response (n=47) planning: IT (96%), Leadership (84%), Compliance (69%).

Literature and Best Practices

Effective incident response requires broad, cross-functional buy-in from all stakeholders across departments. National frameworks (e.g., NIST, HHS 405(d), AHA CLEAR) consistently recommend integrated incident response and business continuity teams, with regular, interdisciplinary tabletop exercises and feedback sessions[17]. High involvement predicts rapid, flexible responses to incidents, faster restoration of operations, and more robust communication during crisis scenarios. Conversely, when incident planning is relegated to a silo (typically IT), data shows gaps in priorities, overlooked workflows, and delayed responses.

While evidence for direct causality between review cycles and incident response success is nuanced, continuous process improvement and regular plan updates are considered fundamental best practices in risk management frameworks (e.g., NIST, HHS, Texas DIR). Regular review cycles provide opportunities to incorporate lessons learned, adapt to regulatory shifts, respond to new threat intelligence, and re-engage key staff. [18] Hospitals that do not engage in cyclical review are outliers and are more likely to have obsolete or untested response plans. [19]

Recommendation

- Formalize regular (at least semi-annual) cross-departmental incident response planning and simulation exercises.
- Clearly define roles and escalation paths for different incident types, ensuring clinical leadership is empowered to make operational decisions during cyber events.
- Actively include Compliance and operational leadership to align technical fixes with HIPAA and Texas DIR regulatory requirements.

[17] U.S. Department of Health & Human Services, 405(d) Program: Health Industry Cybersecurity Practices (HICP) (Washington, DC: HHS ASPR, 2023), https://405d.hhs.gov/.
[18] National Institute of Standards and Technology (NIST), PRISMA – Program Review for Information Security Management Assistance (Gaithersburg, MD: NIST, 2025), https://csrc.nist.rip/prisma/.
[19] California Hospital Association Joint Commission. Emergency Management Update 2024. Chicago: The Joint Commission, September 2024. https://calhospital.org/wp-content/uploads/2024/09/TJC-Emergency-Management-Update-2024-Presentation.pdf.

- Optimal reviews should include multidisciplinary input, recent threat intelligence, and practical simulation feedback.

Effectiveness Perception: Confidence Linked to Process, Not Just Policy

- 65% of respondents (n=38) rate their organization as only being "mostly" prepared for a data breach.

Evidence and Real-World Experience

Staff confidence in response protocols reduces response hesitancy, encourages rapid reporting, and increases compliance with best practices during breach response. Studies corroborate that policies with strong review cycles, inclusive planning, and regular training exercises are viewed as more effective by staff—reinforcing actual security posture. [20] [21]

Hospital leadership should consider that "check-the-box" training and incident planning produce much lower confidence and higher risk than programs that are iteratively improved, carefully explained, and actively practiced across the organization. [22] [23]

Recommendation

- Pair policy updates and review cycles with confidential staff surveys to assess perceived effectiveness and identify knowledge gaps or procedural uncertainties.
- Regularly communicate the "why" behind changes to policy or process, linking new measures to recent threats or lessons learned.

Feedback Mechanisms: Staff Input as a Force Multiplier

- 52% of hospitals (n=22) include some avenue for employee feedback on breach response cybersecurity policy. However, 47% of hospitals (n=20) report that they do not have a way of reporting feedback.

[20] Chelsea Liu and Muhammad Ali Babar, *"Corporate Cybersecurity Risk and Data Breaches: A Systematic Review of Empirical Research," Australian Journal of Management* (2024): 1–31, https://doi.org/10.1177/03128962241293658.
[21] National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide,* Special Publication 800-61 Revision 3 (Gaithersburg, MD: U.S. Department of Commerce, 2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.
[22] Krinken Rohleder, *"Evolving Beyond 'Check-the-Box' Cybersecurity: A Case for Engagement," LinkedIn Pulse,* accessed December 11, 2025, https://www.linkedin.com/pulse/evolving-beyond-check-the-box-cybersecurity-case-krinken-rohleder-rdkmc/.
[23] U.S. Department of Health and Human Services, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,* 405(d) Task Group, 2018, https://405d.hhs.gov/Documents/HICP-Main-508.pdf.

Academic and Practical Rationale

Employee feedback provides critical insights into usability, communication barriers, and overlooked vulnerabilities. Research shows that post-training and post-incident surveys or focus groups identify disconnects between design and operational reality. [24] [25] Organizations with structured feedback loops adapt more rapidly, build trust, and foster a sense of shared mission against cyber threats.

Recommendation

- Implement routine, anonymous post-training and post-incident feedback surveys for all staff.
- Establish regular staff forums (either digital or in-person) for discussing policy and security concerns.
- Empower all employees to suggest improvements or report possible process gaps without fear of reprisal.

Practical Implications for Rural Texas Hospitals

- Among the 32 valid responses, the **majority (84%) reported encountering two or more barriers to implementing cybersecurity improvements**, while 34% reported facing four or more barriers. Of the total sample (n=38), six respondents did not complete this item.

Urgency and Context

Cyberattacks on rural hospitals are particularly prevalent, as these hospitals are particularly vulnerable due to resource constraints, aging infrastructure, and workforce shortages.[26] [27] Attacks can disrupt patient care, delay critical procedures, and erode public trust in healthcare, a direct threat to both financial viability and community safety. The high costs of

[6] Texas Department of Information Resources, *"Statewide Cybersecurity Awareness Training."*
[24] Federal Emergency Management Agency (FEMA), *After Action Review User Guide,* November 2023, https://preptoolkit.fema.gov/documents/d/cip-citap/after_action_review_user_guide_november_2023_f.
[25] Atlassian, *"Post-Incident Review Best Practices," Jira Service Management Cloud Documentation,* accessed December 11, 2025, https://support.atlassian.com/jira-service-management-cloud/docs/post-incident-review-best-practices/.
[26] U.S. Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response (ASPR), *Healthcare System Cybersecurity Readiness & Response Considerations,* ASPR TRACIE, 2018, https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf.
[27] Hannah Neprash, *"Research Insights: Cybersecurity and Healthcare Systems,"* National Institute for Health Care Management (NIHCM), August 1, 2024, https://nihcm.org/assets/articles/FINAL-NIHCM-RI-Hannah-Neprash_2024-08-01-132728_ushq.pdf.

breach remediation, estimated at $1.9M lost per day during hospital downtime, make robust, effective, and relevant security training an existential priority.[28]

Texas' policy landscape emphasizes annual training compliance but offers flexibility in how this goal is achieved.[6] Survey data and recent incident case studies make clear: shifting to a culture of continuous education, simulation, and organizational participation can dramatically reduce breach risks and improve patient outcomes.

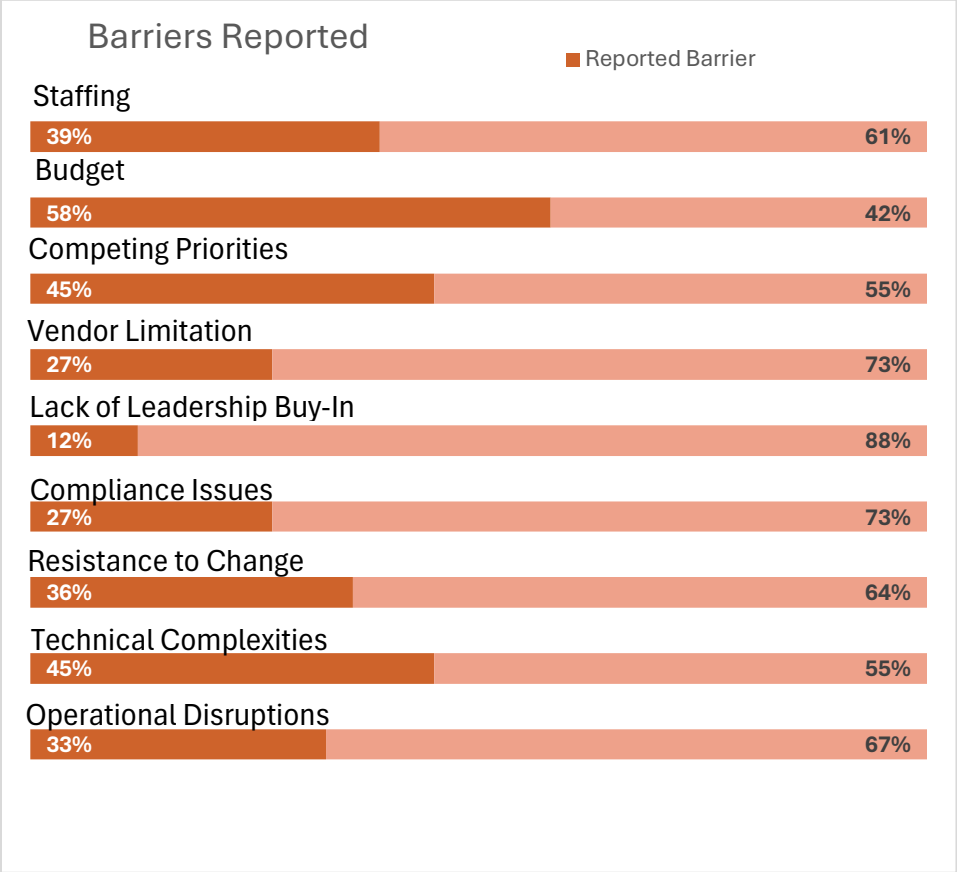

Figure 3 Barriers to Change Respondents Selected (n=32)

Interpreting the Absence of Statistically Significant Findings

While this study aimed to uncover statistically robust patterns in the effectiveness of cybersecurity training across rural Texas hospitals, higher-order statistical testing did not yield significant results. This outcome, though initially disappointing, is not without value. In scientific inquiry, the absence of statistically significant findings is itself a critical data point—one that underscores the importance of transparency, reproducibility, and the iterative nature of research.

[28] Healthcare Financial Management Association (HFMA), *"Ransomware Attacks Drive Up Healthcare Costs," Fast Finance,* accessed December 11, 2025, https://www.hfma.org/fast-finance/ransomware-attacks-healthcare-costs/.

Several factors likely contributed to the lack of statistically significant insights:

- Small Sample Size: The number of participating hospitals and respondents limited the statistical power necessary to detect subtle effects or correlations.
- Accelerated Survey Development Timeline: Due to the urgency of the research the survey instrument was developed and deployed on a compressed schedule, potentially constraining its sensitivity and scope.

Despite these limitations, the survey still yielded valuable descriptive data. Demographic breakdowns, including departmental representation, tenure distributions, and training modality preferences, still offer actionable insights that can inform the design and targeting of future training initiatives. These findings, while not statistically conclusive, provide a directional understanding of where gaps may exist and where interventions could be most impactful.

Recommendations:

1. *Move to Annual PLUS Quarterly Training:*
    - Pair the required annual DIR training with quarterly refreshers or live phishing simulations.
    - Ensure participation is tracked and tied to system access, especially for privileged accounts.
2. *Expand and Blend Content Delivery:*
    - Use a mix of online modules, live workshops, hands-on phishing/email simulations, and written best practice" reminders.
    - Cover new threats and compliance topics, prioritizing high-impact risks for your organization.
    - Leverage zero- or low-cost content from DIR, Microsoft, Google, AHA, and HHS 405(d).
3. *Target Long-Tenured Staff with Role-Specific Refreshers:*
    - Prioritize experienced employees for updated scenario-based refreshers to close knowledge and behavior gaps.
    - Create hospital "cyber ambassadors" among trusted veteran staff to lead by example.

4. *Mandate and Formalize Cross-Departmental Incident Response Planning:*
    - Involve IT, Leadership, Clinical, Operations, and Compliance in exercises and plan reviews.
    - Simulate both technical and business impacts (e.g., downtime procedures, patient diversion strategies).
    - Document and circulate lessons learned after each simulation or real-world incident.
5. *Require Documented Semi-Annual Review Cycles:*
    - Standardize schedule for reviewing and updating incident response, breach, and training policies.
    - Use regulatory and practical metrics to track improvement and compliance.
6. *Institutionalize Anonymous Feedback Loops:*
    - Use anonymous surveys after training or incident simulations to capture gaps, confusion, and practical suggestions.
    - Set up regular feedback forums and include representative staff from all shifts and roles.
7. *Leverage State and Federal Support:*
    - Apply for grants that support tailored cybersecurity initiatives for rural hospitals (e.g., Microsoft, Google, CISA, federal HRSA programs).
    - Partner with regional cybersecurity support centers and peer hospital networks for knowledge sharing and incident response coordination.
8. *Integrate Cybersecurity with Organizational Strategy:*
    - Recognize cyber risk as a core business (not IT-only) challenge tied to patient safety, continuity of service, and financial sustainability.
    - Mobilize CEOs and governing boards to champion ongoing investments in security training and infrastructure.

Conclusion

Rural hospitals in Texas are the backbone of rural healthcare, and increasingly, the frontline in an ongoing battle against sophisticated cyber threats. Survey data and the latest research make clear: training programs that are infrequent, static, or siloed leave hospitals and their patients exposed. Annual compliance must evolve into an evidence-based and frequently refreshed approach, supported by departmental involvement, routine plan reviews, and staff ownership.

Transitioning to a blended, feedback-driven model not only improves breach response but also fosters institutional resilience and confidence in the face of rising threats. With support from state and national partners, and by prioritizing investments in workforce development and cross-functional collaboration, rural Texas hospitals can achieve cyber maturity and continue to serve their communities safely and reliably for years to come.

Source:

Atlassian. *"Post-Incident Review Best Practices." Jira Service Management Cloud Documentation*. Accessed December 11, 2025. https://support.atlassian.com/jira-service-management-cloud/docs/post-incident-review-best-practices/.

California Hospital Association Joint Commission. *Emergency Management Update 2024*. Chicago: The Joint Commission, September 2024. https://calhospital.org/wp-content/uploads/2024/09/TJC-Emergency-Management-Update-2024-Presentation.pdf.

Chief Healthcare Executive. *"Ransomware Attacks Threaten Rural Hospitals: HIMSS 2025."* Chief Healthcare Executive, 2025. https://www.chiefhealthcareexecutive.com/view/ransomware-attacks-threaten-rural-hospitals-himss-2025.

Cookey, I. B., C. M. Ajoku, and P. B. Ogini. *"Security Awareness and Phishing Training in Nigerian Institutions." International Journal of Scientific Research in Education* 18, no. 2 (2025). Accessed December 10, 2025. https://ijsre.com.ng/assets/vol.%2c-18%282%29-cookey%2c-i.-b.%2c-ajoku%2c-c.-m.%2c---ogini%2c-p.-b.pdf.

Federal Emergency Management Agency (FEMA). *After Action Review User Guide*. November 2023. https://preptoolkit.fema.gov/documents/d/cip-citap/after_action_review_user_guide_november_2023_f.

Frati, Fulvio, Georgiana Darau, Nikos Salamanos, and Pantelitsa Leonidou. *"Cybersecurity Training and Healthcare: The AERAS Approach." International Journal of Information Security* 23, no. 2 (January 2024): 1–13. https://doi.org/10.1007/s10207-023-00802-y.

GTIA North America Cybersecurity Interest Group. *Tabletop Exercises to Build Customer Resilience and Preparedness*. GTIA, 2025. https://gtia.org/hubfs/GTIA%20Cybersecurity%20Guidebook%20for%20ITSPs%20-%20Tabletop%20Exercises.pdf.

Healthcare Financial Management Association (HFMA). *"Ransomware Attacks Drive Up Healthcare Costs." Fast Finance*. Accessed December 11, 2025. https://www.hfma.org/fast-finance/ransomware-attacks-healthcare-costs/.

HIPAA Journal. *"Microsoft Cybersecurity Rural Hospital Program 2025 Update."* HIPAA Journal, 2025. https://www.hipaajournal.com/microsoft-cybersecurity-rural-hospital-program-2025-update/.

Ho, Grant, Adriana Mirian, et al. *Phishing Training Effectiveness: Evidence from Oakland 2025*. University of Chicago, 2025. Accessed December 10, 2025. https://people.cs.uchicago.edu/~grantho/papers/oakland2025_phishing-training.pdf.

Jacobs, Jody L., Julie M. Haney, and Susanne M. Furman. *Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study.* Gaithersburg, MD: National Institute of Standards and Technology, 2021. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934952.

Jayatilaka, Asangi, Nathan Beu, Irina Baetu, Mansooreh Zahedi, M. Ali Babar, Laura Hartley, and Winston Lewinsmith. *"Evaluation of Security Training and Awareness Programs: Review of Current Practices and Guidelines."* arXiv preprint arXiv:2112.06356 (2021). https://arxiv.org/pdf/2112.06356.

KnowBe4. *"KnowBe4 Research Confirms Effective Security Awareness Training Significantly Reduces Data Breaches."* Press release. Accessed December 10, 2025. https://www.knowbe4.com/press/knowbe4-research-confirms-effective-security-awareness-training-significantly-reduces-data-breaches

Liu, Chelsea, and Muhammad Ali Babar. *"Corporate Cybersecurity Risk and Data Breaches: A Systematic Review of Empirical Research." Australian Journal of Management* (2024): 1–31. https://doi.org/10.1177/03128962241293658.

Liu, Lin, et al. *Understanding the Efficacy of Phishing Training in Practice.* University of Chicago & UC San Diego, 2025. https://people.cs.uchicago.edu/~grantho/papers/oakland2025_phishing-training.pdf.

National Institute of Standards and Technology (NIST). *Computer Security Incident Handling Guide.* Special Publication 800-61 Revision 3. Gaithersburg, MD: U.S. Department of Commerce, 2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

National Institute of Standards and Technology (NIST). *PRISMA – Program Review for Information Security Management Assistance.* Gaithersburg, MD: NIST, 2025. https://csrc.nist.rip/prisma/.

National Rural Health Association. *Cybersecurity and Rural Health Policy Brief.* 2024. https://www.ruralhealth.us/getmedia/ad0774a2-49b4-4f9a-b2c5-2edf0eaf6bcf/2024-NRHA-Cybersecurity-Rural-Health-policy-brief.pdf.

Neprash, Hannah. *"Research Insights: Cybersecurity and Healthcare Systems."* National Institute for Health Care Management (NIHCM), August 1, 2024. https://nihcm.org/assets/articles/FINAL-NIHCM-RI-Hannah-Neprash_2024-08-01-132728_ushq.pdf.

Reeves, A., P. Delfabbro, and D. Calic. *"Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue." SAGE Open* 11, no. 2 (2021). https://journals.sagepub.com/doi/pdf/10.1177/21582440211000049.

Rohleder, Krinken. *"Evolving Beyond 'Check-the-Box' Cybersecurity: A Case for Engagement."* *LinkedIn Pulse*. Accessed December 11, 2025. https://www.linkedin.com/pulse/evolving-beyond-check-the-box-cybersecurity-case-krinken-rohleder-rdkmc/.

Rural Health Information Hub. *Cybersecurity Toolkit for Rural Hospitals and Clinics*. 2024. https://www.ruralcenter.org/sites/default/files/Cybersecurity%20Toolkit%20for%20Rural%20Hospitals%20and%20Clinics.pdf.

Texas Department of Information Resources (DIR). *"Statewide Cybersecurity Awareness Training."* Accessed December 11, 2025. https://dir.texas.gov/information-security/statewide-cybersecurity-awareness-training.

Texas Recap. *"Massive Cyberattack Hits Texas Hospital Network, Patient Data Compromised."* Texas Recap, 2025. https://texasrecap.com/massive-cyberattack-hits-texas-hospital-network-patient-data-compromised/.

U.S. Department of Health & Human Services. *"HIPAA Training and Resources."* HHS.gov, 2025. https://www.hhs.gov/hipaa/for-professionals/training/index.html.

U.S. Department of Health & Human Services. *405(d) Program: Health Industry Cybersecurity Practices (HICP)*. Washington, DC: HHS ASPR, 2023. https://405d.hhs.gov/.

U.S. Department of Health & Human Services. *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. 405(d) Task Group, 2018. https://405d.hhs.gov/Documents/HICP-Main-508.pdf.

U.S. Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response (ASPR). *Healthcare System Cybersecurity Readiness & Response Considerations*. ASPR TRACIE, 2018. https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

J. Chialastri (2025) Cybersecurity Training Effectiveness in Texas Rural Hospitals for Texas Hospital Association. Institute for Homeland Security.

https://doi.org/10.17605/OSF.IO/C9234