Losing What We Know:

Organizational Forgetting as a Pathway to Normalized Deviance in Critical Infrastructure Organizations

WRITTEN BY

Alexander Kinney, Ph.D

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

ABSTRACT

Critical infrastructure organizations increasingly face workforce transitions leading to a loss of accumulated institutional knowledge. This is also known as “organizational forgetting.” Existing research has examined factors leading to these losses, including retirements, outsourcing, and routine organizational turnover. Yet the consequences of knowledge loss are largely understood in terms of performance outcome.

Organizations typically focus on productivity and efficiency. They don’t often consider how knowledge loss, especially over time, changes how we interpret warning signs and calculate acceptable risk.

This paper explores the issue by considering how institutional knowledge loss may degrade our organizational capacity to identify and respond to threats.

- It first reviews the existing research on organizational forgetting. This allows us to identify several pathways through which knowledge loss may reshape organizational definitions of acceptable risk.
- It then draws on “normalization of deviance” literature to consider how continued operation in the face of knowledge loss may reinforce perceptions that emerging threats or risks are considered safe.
- Finally, it highlights opportunities for critical infrastructure organizations to strengthen knowledge-retention as a key strategy for risk management.

Table of Contents

INTRODUCTION AND OVERVIEW **1**
The Growing Risk of Organizational Knowledge Loss 1

GAP ASSESSMENT/PROBLEM STATEMENT **2**
Research Objective 2

TOPIC DISCUSSION **3**
Uncovering the Sources of Organizational Forgetting 3
Expected Employee Departures as a Key Source of Organizational Forgetting 4
Outsourcing and Losing Knowledge to External Stakeholders 5
Organizational Forgetting as a Pathway to Normalized Deviance 6

WAY FORWARD **8**
Implement practices to identify information whose loss would impair risk decisions. 8
Develop protocols to preserve the reasoning behind consequential decisions. 9
Create structured opportunities for information sharing. 9
Continuously test the usability of transferred knowledge. 10

CONCLUSION **10**

REFERENCES **11**

INTRODUCTION AND OVERVIEW

The Growing Risk of Organizational Knowledge Loss

There are over 16.6 million people employed in infrastructure-related occupations in the United States (Kane, 2022). Of these employees, approximately 86.8% need some form of on-the-job training (Kane, 2022). This places a significant demand on organizational resources.

Changing regulations and evolving technology also place new pressures on organizational continuity.

Because many critical infrastructure employers tend to rely on specialized knowledge developed over years of experience, small shifts in the composition of the workforce can have a drastic impact on how knowledge gets transferred to new workers. Kane (2022) projects that approximately 1.7 million critical infrastructure workers will leave the labor force or move into a different occupational field annually between 2021 and 2031.

Taken together, this level of workforce attrition coupled with the prevalence of on-the-job training suggests that knowledge transfer in critical infrastructure organizations should remain a key area of concern for managers.

This real-world dynamic also suggests that critical infrastructure organizations are also more at risk of confronting an issue known to researchers as "organizational forgetting" (de Holan and Phillips, 2004b), where separations from organizations place distance between an organization and the key sources of knowledge that are crucial to everyday operations. Though there is always the ever-present concern that there will not be enough workers available to fill vacant positions, critical infrastructure organizations in particular must now consider whether the *types* of workers they recruit will provide individuals with accumulated expertise to be trained effectively, so that they can perform their work safely. Though some optimism has emerged in recent years that federal infrastructure investments could create new opportunities for employment and training programs (see Mortiere et al., 2025), these are stop-gap efforts that do not automatically replace the rich reservoir of "tacit" or informal expertise that leaves when employees depart from an organization (Ambrosini & Bowman, 2001), or when work tasks are outsourced to external stakeholders (Edvardsson & Durst, 2019).

Organizational forgetting also has downstream effects on routines in critical infrastructure organizations. Beyond the reality that a substantial portion of operational knowledge is difficult to capture in formal repositories (Easterby-Smith & Lyles, 2011), researchers point to larger concerns about the downstream impacts of institutional knowledge loss in organizational culture. When experienced employees depart an organization, the organization can lose the ability to identify which knowledge losses are truly concerning and how to respond (Ambrosini & Bowman, 2001; DeLong, 2004). Consequently, when critical infrastructure organizations lose

employees who can help develop appropriate judgment in their replacements, this can have collateral consequences for safety that only reveal themselves once disaster strikes (Vaughan, 1996; Vaughan, 1999; Vaughan, 2004; Vaughan, 2021).

GAP ASSESSMENT/PROBLEM STATEMENT

Research on organizational forgetting traditionally examines its effects on performance (see Massingham, 2018). However, research has focused less on understanding how lost knowledge can change the way that employees interpret anomalies or how they define acceptable risk over time. This paper considers the loss of knowledge in organizations as a factor that contributes to "normalization of deviance" (Vaughan, 1996). "Normalization of deviance occurs when the definition of acceptable risk in organizations gradually shifts over time to the point that employees casually engage in practices that can lead to catastrophic outcomes."

Lost knowledge does not automatically cause this process. However, it removes a crucial source of context employees rely upon to develop a shared understanding of safety that leads to safe operating conditions. This includes information about:

- why certain safeguards were developed (DeLong, 2004).
- why earlier anomalies may have generated outsized concern among key stakeholders (Vaughan, 1996)., or
- why continuing to operate in the face of such anomalies should not always be interpreted as evidence that existing practices are safe (Dillon, Tinsley, & Burns, 2014).

This type of background knowledge is helpful in risk assessments. And when relevant experience is lost, it becomes harder to even evaluate work conditions (Aven, 2012). Thus, it is important to see workforce management issues and operational risk as things to manage collectively, rather than as separate dynamics that independently contribute to potential adverse outcomes.

Research Objective

This paper expressly considers knowledge loss as a risk-management problem central to critical infrastructure resilience. Specifically, it considers (1) how retirements, turnover, and employee outsourcing can contribute to organizational forgetting, and (2) how knowledge-transfer practices can preserve or fail to preserve the context needed for workers to properly identify anomalies. In doing so, this paper connects the conditions of organizational forgetting to normalization of deviance framework (see Vaughan, 1996; Vaughan, 1999; Vaughan, 2004) to offer practical strategies that critical infrastructure organizations can use to mitigate potential consequences associated with organizational forgetting.

TOPIC DISCUSSION

Uncovering the Sources of Organizational Forgetting

It is important to recognize that there is a distinction between what we can write down and what must people must learn on the job. This distinction commonly captured in the academic literature through the concepts of "explicit" and "tacit" knowledge (Smith, 2001).

Explicit knowledge is expressed in common organizational artifacts. These include written procedures and training materials that serve as the backbone of operational continuity across the organizational life course. Tacit knowledge, on the other hand, is more difficult to formalize because it emerges from, and is shaped by, daily practice (Easterby-Smith & Lyles, 2011).

Tacit knowledge includes the ability to recognize when a proprietary instrument is behaving unusually, or to know which employee on a team is uniquely equipped with the requisite experience to resolve an unfamiliar problem. Though you can uncover tacit knowledge through interviews and observations of organizational culture, it is challenging to disentangle it from the activity where it is deployed. This makes tacit knowledge difficult to identify by even the most skilled managers and consultants (Ambrosini & Bowman, 2001).

Complicating this issue is the reality that organizational knowledge also exists in various technologies, routines, processes, and relationships (Argote, 2012). For instance, many critical infrastructure employees will not only learn how to operate equipment during their occupational tenure, but they will also learn how that equipment behaves under certain conditions through experience and training. In time, they will come to know different responsibilities are attached to their job role, and which coworkers can be relied upon when they encounter a novel issue. Finally, they will develop a nuanced familiarity with formal procedures that, over time, will become second nature. This allows them to understand when those procedures may not fully account for conditions they observe in real time.

Vaughan's (2021) study of air traffic control provides a useful illustration of how this process unfolds in a critical infrastructure setting. Setting out to understand how controllers safely manage air traffic so that little mistakes do not always spiral into catastrophes, Vaughan found that employees rely on a combination of formal rules, automated systems, and standardized communication routines to coordinate aircraft movement. However, perhaps less obviously, she also discovered that the ability to apply these resources requires careful collaboration between controllers over extended time periods. Experienced controllers learn to anticipate how conditions may evolve into a catastrophic outcome before an obvious threat emerges. Apprenticeships are crucial for onboarding new controllers so that they can glean this tacit knowledge, with trainings lasting anywhere from several months at a specific airport to several years across regional centers. During this period, employees learn to coordinate with others in an environment where available information can change meaning rapidly. When we think about

expertise in this respect, Vaughan shows us that it might be better understood as something existing within a collective workforce rather than an attribute possessed by specific employees.

If expertise is sustained through routine interactions between employees, respective operational technologies, and the organizational environment, then losing knowledgeable workers interrupts the very process through which organizations reproduce expertise. In other words, separations represent a key form of "organizational forgetting" whereby knowledge that may have been widely available within an organization suddenly becomes inaccessible, or at the very least, difficult to recover (de Holan & Phillips, 2004b).

Organizational forgetting can offer strategic advantages when organizations deliberately discard knowledge that is no longer considered useful. However, knowledge loss can also arise unintentionally through routine operations and can present profound problems for organizational planning (de Holan and Phillips, 2004a). Importantly, this loss can occur through several avenues: retirement, routine turnover, outsourcing, and ineffective knowledge transfer practices before employees leave (DeLong, 2004; Galan, 2023a, Galan 2023b). Though each pathway affects this process in a unique way, they all share a common outcome of eroding the collective judgment to use formal procedures and systems effectively. Examining each of these pathways can reveal different points where knowledge can become detached from the people and practices that critical infrastructure organizations depend upon to operate in a safe manner.

Expected Employee Departures as a Key Source of Organizational Forgetting

There are two common ways employee departures contribute to institutional knowledge loss in critical infrastructure organizations: employee retirements (DeLong, 2004) and routine job turnover (Galan, 2023a). Retirements are one of the more predictable pathways to this outcome as they are largely foreseeable events organizations can plan for, allowing them to identify who is leaving and when. Despite this, *advance notice does not necessarily uncover the full scope of knowledge that is at risk of disappearing*. Retiring employees often accumulate decades of experience that translates into a nuanced understanding of everything from the history of equipment failures to a understanding why certain practices were implemented when they were (DeLong, 2004). One of the biggest challenges confronting critical infrastructure organizations in coming decades will be in developing methods to support knowledge transfer from an increasingly aging workforce. This will help them better buffer against organizational forgetting (Burmeister & Deller, 2016; Kane, 2022).

A major factor in the successful transfer of this knowledge is incentivizing experienced employees to communicate their knowledge to other employees, creating an organizational culture where newer employees are personally invested in learning, and promoting opportunities for sustained interaction between these parties. Exit interviews and documentation are one way to preserve some of this valuable expertise, but without proper relationship building these artifacts may be misinterpreted. Moreover, even when knowledge is shared before an employee

departs, an organization has not necessarily retained it unless current employees can access and apply it in their own job roles (Galan, 2023b). Retirements, therefore, create a specific type of risk for critical infrastructure organizations. Organizations may be aware of departures, but not be fully aware of the knowledge that will disappear along with the employee or if the relationships needed to preserve that knowledge have been sufficiently established.

Routine employee turnover is a more insidious force than planned retirements. Organizations expect people to regularly move in and out of job roles. That said, who or when someone is likely to leave, or what knowledge disappear with them, can be unpredictable. Galan's (2023a) systematic review of the research found that the consequences of this type of turnover are idiosyncratic. Seniority in departures, of course, matters. But even workers with shorter tenures can still have specialized knowledge that disrupts organizational capacities when they depart from the organization. This means repeated turnover is a persistent threat to institutional knowledge retention.

In critical infrastructure organizations, this presents unique challenges. Hiring a replacement for a departing worker may bring a unit or team back to full numbers but may not immediately reconstruct the departing worker's experience or the respect previously endowed to the role by leadership. Moreover, because departures are treated as a routine element of organizational life, each instance rarely generates concern on its own. This can mask the cumulative impact of turnover on operations. While retirement offers a more visible form of departure that organizations can plan for, routine personnel changes facilitate a gradual disappearance of organizational knowledge that is more difficult to respond to.

Outsourcing and Losing Knowledge to External Stakeholders

Outsourcing is another avenue of organizational forgetting where expertise gets transferred to an outside source (Edvardsson & Durst, 2019). There are practical reasons why organizations might pursue outsourcing as a broader operational strategy, including reducing costs or allowing an organization to access specialized forms of expertise that might be difficult to develop internally. However, these benefits can come at a different type of cost: when organizations outsource key tasks to external workers, the internal workforce loses out on opportunities to develop knowledge that comes from direct engagement with tasks. The organization may retain formal authority and responsibility for how an activity <u>is</u> carried out while gradually losing firsthand experience that promotes a greater technical understanding of how that activity <u>should be</u> carried out.

When critical infrastructure organizations outsource core functions, there is a risk that their capacity to anticipate or respond to failures will erode over time (Edvardsson and Durst, 2019). Outsourcing does not shield the internal organization from failures that emerge from the actions of the contractor. This means that negative consequences can still cascade across the larger operational system. A less obvious consequence is that the knowledge of how problems are solved is transferred to outside of the organization to contractors. When these contractors take a

leading role in responding to these failures, they may develop vital, firsthand knowledge about why the failure occurred and how it was resolved. With "outsiders" addressing failures, the organization can lose knowledge of how the contractor solved the problem unless the organization's response includes deliberate opportunities to share and apply what the contractor learned (Edvardsson & Durst, 2019).

This can make it more difficult for organizations to access information they could use for process improvement. Ultimately, the more an organization comes to depend on outsourced support, the more precarious their position becomes. They are in the position of having to shoulder the burden of responsibility for managing the consequences of these failures without the requisite knowledge to understand whether work can safely resume.

Organizational Forgetting as a Pathway to Normalized Deviance

The preceding section identifies several ways organizations can lose expertise and how that loss affects decision-making. This section turns to the literature in the sociology of disasters to advance the argument that decisions should be viewed as collective organizational output in situations where danger is not obvious to everyone involved (Vaughan, 1996). This research suggests that navigating dangerous situations requires employees to:

1. Remain vigilant to the possibility of failure being right around the corner.
2. They should exercise a cautionary stance in routine decision making (Weick & Sutcliffe, 2001).

Though these are often framed as principles inherent to a strong organizational culture, this culture rarely exists when organizational expertise is lacking or undergoes suddenly changes. A cautionary stance is difficult to maintain when employees are neither able to recognize conditions that precede failure, nor if experienced peers are difficult to find due to outsourcing. Knowledge loss may make employees more likely to view the absence of an obvious adverse outcome as evidence that work conditions are safe, instead of routinely questioning whether on-the-ground conditions warrant concern (Vaughan, 1996).

One common way to view this issue firsthand is through the concept of "near misses." These occur when a harmful outcome was narrowly avoided without reviewing and clarifying whether existing protections worked as intended or the organization was fortunate to escape a failure (Dillon et al., 2014). In critical infrastructure organizations, a piece of equipment might, for instance, begin to behave unusually during routine operations, but continue to function normally once an experienced worker intervenes. If no failure is recorded and work proceeds, this event may be interpreted by employees in different ways. For some employees, this event may be remembered as a moment where equipment was on the brink of failure until someone recognized a developing problem and acted on it before it became serious. However, for other employees that are only aware that the equipment kept running, the same event might be interpreted as

evidence that its behavior fell within acceptable limits. When knowledge of an intervention and why the worker considered it necessary is not documented, different employees may be unable to tell which kind of event occurred or which type of interpretation more accurately characterizes it. Over time, continued operations become evidence of safety even when they follow interventions that may not always occur.

The interpretation of near misses can have consequences beyond the event itself. When teams view continued operation as evidence of safe working conditions, this judgment can inform later decisions about what operating conditions are acceptable. Vaughan's (1996) study of the Challenger disaster showed how this can happen through even the most ordinary of organizational decisions. Though engineers and managers observed damage to the shuttle's critical components on earlier flights, they evaluated this damage through established procedures and sanctioned future flights. Because these earlier flights did not lead to catastrophe, their outcomes helped to support judgments that this damage could be considered an acceptable risk.

This gradual shift from "concern" to what is treated as "normal" highlights how near misses interpreted as evidence of safety can contribute to the "normalization of deviance" in critical infrastructure organizations (Vaughan, 1999; Vaughan, 2004). Vaughan's work shows that, in addition to employees becoming desensitized to warnings, production demands and fragmented information access can shape which warning signs an organization treats as credible threats. Knowledge loss may make it harder for employees to challenge the resulting judgments when the experience behind earlier concerns is no longer available (DeLong, 2004).

Ultimately, what this work demonstrates is how continued operation can strengthen confidence in established practice, even as organizations lose the knowledge needed to question it. The decisions that determine which warning signs become accepted, and why, can outlast employees who made them. Turnover can make it more difficult to sustain the collective knowledge that employees depend on to understand when earlier judgment calls should be reevaluated (Anderson & Lewis, 2014). This is how organizational forgetting can reinforce this process without being its sole cause (Vaughan, 1996; Vaughan, 1999; Vaughan, 2004). When operations continue without an obvious failure, that outcome can support an interpretation that the organization is making sound judgment calls. But as Dillon et al. (2014) demonstrate, *a lack of failure alone is not enough to establish how close to catastrophe an event was or what employees should learn from it*. In tandem with the research on organizational forgetting, the sociology of disaster literature shows us that preserving access to rationales behind earlier decisions matters nearly as much as documenting what decision was made. Over time, without proper protocols in place to preserve these rationales, organizations may silently lose the capacity to critically evaluate why earlier judgments were made when experienced people leave the organization.

WAY FORWARD

Thus far, the paper has established that:

- Organizational forgetting is a practical challenge that can follow planned separations, such as retirements and outsourcing, as well as unexpected employee departures.
- Expected organizational responses to knowledge loss stemming from these separations, (such as replacing departing workers or preserving written procedures) do not, on their own, protect an organization from potential adverse outcomes associated with risk evaluation.

This is why traditional organizational responses to knowledge loss are only a baseline for preventing redefining acceptable risk over time. They should be built on to further limit knowledge loss.

Based on current practices and the literature reviewed, following are four ways critical infrastructure organizations can create more robust responses to organizational forgetting. These couple insights from these respective literatures into existing, or future, organizational practice.

Implement practices to identify information whose loss would impair risk decisions.

Critical infrastructure organizations need to establish, in concrete terms, what they would have difficulty evaluating or explaining if a key stakeholder suddenly became unavailable (Burmeister & Deller, 2016; Galan, 2023b). By taking stock of which operating histories are understood by few employees, figuring out which tasks commonly require extended experience to master, or identifying core relationships within the organization that come to bear on resolving problems, critical infrastructure organizations can become more resilient. A tool that offers a practical starting point for this task is a knowledge map (Wexler, 2001). Knowledge maps take the form of textual and/or visual diagrams that document these key dimensions of organizational knowledge so that existing and future employees have a shared resource to understand who to go to, and importantly, why in specific moments of organizational action. A knowledge map might identify who understands the history of a particular piece of equipment, including when it has acted out of character and how these moments were resolved. It might also identify where earlier investigations are documented or offer directions as to which organizational contact might have the most diagnostic expertise. Knowledge maps make connections visible, creating a key record of information that supplements protocols and procedures. They also take into account specific factors that affect organizational learning like expected and unexpected employee departures. Critical infrastructure organizations may consider consulting industry associations for sector-specific knowledge-mapping tools.

Develop protocols to preserve the reasoning behind consequential decisions.

By the nature of their work, critical infrastructure organizations will confront unusual work conditions. When these conditions appear, any record of decision-making should include an explanation of what prompted concerns and how these concerns were resolved. Incident investigations are recommended by federal agencies (see Occupational Safety and Health Administration, 2016). OSHA recommends investigating both harmful incidents and near misses to identify shortcomings in safety programs. It is recommended that organizations develop a formalized way to conduct reviews of near-miss incidents to document successful (and unsuccessful) interventions, the types of evidence that were evaluated in the decision-making process, the alternative interpretations of the event that were considered, and what uncertainty remained. As Dillon et al. (2014) note, treating a near miss incident as evidence that an organization is resilient could lead to a systematic underestimation of danger in the future. Preserving the full scope of rationales behind decisions allows future employees to evaluate whether earlier judgment calls remain applicable (Vaughan, 1996). The goal of this recommendation is to reduce the possibility that in-the-moment decisions to accept deviations from established precedent will feed into a culture of normalizing deviance across the organization (Vaughan, 1999; Vaughan, 2004).

Create structured opportunities for information sharing.

Employees need opportunities to learn from experienced colleagues how to recognize warning signs and decide when intervention is necessary (Vaughan, 2021). Instead of allowing these teaching moments to proceed in an unstructured fashion, critical infrastructure organizations should create formal opportunities to share knowledge that promote longer-term collaborations. One tool to employ this approach is known as a Cognitive Demands Table which organizes findings from debriefing interviews with experts (see Militello and Hutton, 1998). This is a short worksheet that is filled out after the resolution of an anomalous event in a collective fashion. Critical infrastructure organizations may consider adapting this format for joint interviews with experienced employees and novice colleagues to examine a resolved anomaly. They might work together to record what judgment was applied to the situation, why it was a difficult decision to make, what cues the experienced employee used to make that decision, and potential mistakes that less experienced colleagues might make. Over time, these tables can accumulate into a resource bank that is available to teams as their compositions shift. Such a resource bank could offer a valuable record of tacit knowledge that more often goes unaccounted for in procedural artifacts (Easterby-Smith & Lyles, 2011). Moreover, supervisors can use these completed worksheets to guide training, giving them real-world examples that employees in the organization have confronted, rather than purely rely on imagined scenarios.

Continuously test the usability of transferred knowledge.

One approach to strengthening knowledge preservation efforts is to routinely evaluate whether employees can quickly and accurately apply transferred information. As Galan (2023b) asserts, completing the handover process should be the first step in knowledge transfer, not the concluding operation. Equipment, personnel, and importantly, work conditions will change over time which means that organizations need to continuously assess whether employees can explain rationales for practices such as why a safeguard exists or why an earlier response is no longer relevant to a situation. In addition to common observational practices that managers engage in, there are publicly available tools that can assist critical infrastructure organizations in this effort. For instance, FEMA's Exercise Evaluation Guides (EEGs) offer a structured approach to evaluating organizational performance against defined objectives that critical infrastructure organizations could adapt to assess the usability of transferred knowledge (see FEMA, n.d.). Organizations can also consult with sector-specific industry associations for more localized, tailored guidance.

CONCLUSION

Organizational forgetting is a persistent challenge for critical infrastructure organizations. Also, organizational separations change the types of expertise available in operational decision-making situations. Therefore, personnel separations are a key avenue by which the capacity to evaluate safe work conditions changes over time. This contributes to the gradual redefinition of what constitutes acceptable risk in an operational environment. We suggest four opportunities to address knowledge loss. These offer several practical starting points for critical infrastructure organizations to strengthen knowledge retention in ways appropriate their specific needs. By incorporating these practices, critical infrastructure organizations can better preserve expertise needed to identify emerging threats.

REFERENCES

Ambrosini, V., & Bowman, C. (2001). Tacit Knowledge: Some Suggestions for Operationalization. *Journal of Management Studies*, *38*(6), 811–829. https://doi.org/10.1111/1467-6486.00260

Anderson, E. G., & Lewis, K. (2014). A Dynamic Model of Individual and Collective Learning Amid Disruption. *Organization Science*, *25*(2), 356–376. https://doi.org/10.1287/orsc.2013.0854

Argote, L. (2012). *Organizational learning: Creating, retaining and transferring knowledge*. Springer Science & Business Media. https://books.google.com/books?hl=en&lr=&id=lro1J_ISmesC&oi=fnd&pg=PR5&dq=Organizational+learning:+Creating,+retaining+and+transferring+knowledge+(2nd+ed.).+Springer.&ots=vru2jE9qFq&sig=t5d2xSOytd8dLf8o6zgkZ88GMBo

Aven, T. (2012). Foundational Issues in Risk Assessment and Risk Management. *Risk Analysis*, *32*(10), 1647–1656. https://doi.org/10.1111/j.1539-6924.2012.01798.x

Burmeister, A., & Deller, J. (2016). Knowledge retention from older and retiring workers: What do we know, and where do we go from here? *Work, Aging and Retirement*, *2*(2), 87–104.

De Holan, P. M., & Phillips, N. (2004a). Organizational forgetting as strategy. *Strategic Organization*, *2*(4), 423–433. https://doi.org/10.1177/1476127004047620

De Holan, P. M., & Phillips, N. (2004b). Remembrance of Things Past? The Dynamics of Organizational Forgetting. *Management Science*, *50*(11), 1603–1613. https://doi.org/10.1287/mnsc.1040.0273

DeLong, D. W. (2004). *Lost knowledge: Confronting the threat of an aging workforce*. Oxford University Press. https://books.google.com/books?hl=en&lr=&id=v8aHOQnOXgQC&oi=fnd&pg=PR9&dq=Lost+knowledge:+Confronting+the+threat+of+an+aging+workforce.+Oxford+University+Press.&ots=4B0zBhek4Q&sig=LgkKCZ2qHLz1sDt8ho_wyxD_yPc

Dillon, R. L., Tinsley, C. H., & Burns, W. J. (2014). Near-Misses and Future Disaster Preparedness. *Risk Analysis*, *34*(10), 1907–1922. https://doi.org/10.1111/risa.12209

Easterby-Smith, M., & Lyles, M. A. (Eds.). (2011). Handbook of organizational learning and knowledge management. John Wiley & Sons. https://books.google.com/books?hl=en&lr=&id=9spxuzAIc2QC&oi=fnd&pg=PA19&dq=Handbook+of+organizational+learning+and+knowledge+management&ots=fj0s9YZYME&sig=30wcQmQOgqqgEOkweF1b5UaKZiA

Edvardsson, I. R., & Durst, S. (2019). The Impact of Outsourcing on Knowledge and Learning in Organizations. In L.-P. Dana & V. Ratten (Eds.), *Societal Entrepreneurship and Competitiveness*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-83867-471-720191012

FEMA. (n.d.). *Exercise Evaluation Guides—HSEEP Resources—Preparedness Toolkit*. HSEEP Resources. https://preptoolkit.fema.gov/web/hseep-resources/eegs

Galan, N. (2023a). Knowledge loss induced by organizational member turnover: A review of empirical literature, synthesis and future research directions (Part I). *The Learning Organization: An International Journal*, *30*(2), 117–136. https://doi.org/10.1108/TLO-09-2022-0107

Galan, N. (2023b). Knowledge loss induced by organizational member turnover: A review of empirical literature, synthesis and future research directions (Part II). *The Learning Organization*, *30*(2), 137–161.

Kane, J. W. (2022). Seizing the US infrastructure opportunity: Investing in current and future workers. *Washington DC: Brookings.* https://internationalpolicybrief.org/wp-content/uploads/2023/10/ARTICLE5-183.pdf

Massingham, P. R. (2018). Measuring the impact of knowledge loss: A longitudinal study. *Journal of Knowledge Management*, *22*(4), 721–758.

Militello, L. G., & Hutton, R. J. B. (1998). Applied cognitive task analysis (ACTA): A practitioner's toolkit for understanding cognitive task demands. *Ergonomics*, *41*(11), 1618–1641. https://doi.org/10.1080/001401398186108

Mortiere, P., Johnson, M., DeRenzis, B., & LaPrad, J. (2025). Building the Future Workforce: A State Playbook to Shape a New Age in Federal Infrastructure Investments. *National Skills Coalition*. https://eric.ed.gov/?id=ED671307

Occupational Safety and Health Administration. (2016). Recommended practices for safety and health programs. *Occupational Safety and Health Administration: Washington, DC, USA*.

Smith, E. A. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of Knowledge Management*, *5*(4), 311–321.

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago press. https://books.google.com/books?hl=en&lr=&id=6f6LrdOXO6wC&oi=fnd&pg=PR9&dq=The+Challenger+launch+decision:+Risky+technology,+culture,+and+deviance+at+NASA.+University+of+Chicago+Press.&ots=ygR_BiVHKS&sig=njUqu4ixMZyGBOz3-0UCV-sN8Xo

Vaughan, D. (1999). THE DARK SIDE OF ORGANIZATIONS: Mistake, Misconduct, and Disaster. *Annual Review of Sociology*, *25*(1), 271–305. https://doi.org/10.1146/annurev.soc.25.1.271

Vaughan, D. (2004). Theorizing Disaster: Analogy, historical ethnography, and the Challenger accident. *Ethnography*, *5*(3), 315–347. https://doi.org/10.1177/1466138104045659

Vaughan, D. (2021). Dead reckoning: Air traffic control, system effects, and risk. University of Chicago Press. https://www.degruyterbrill.com/document/doi/10.7208/chicago/9780226796543/html

Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected* (Vol. 9). San Francisco: Jossey-Bass. https://www.researchgate.net/profile/Kathleen-Sutcliffe/publication/265106124_Managing_the_Unexpected_Resilient_Performance_in_an_Age_of_Uncertainty/links/55e83a4308aeb6516262fe22/Managing-the-Unexpected-Resilient-Performance-in-an-Age-of-Uncertainty.pdf

Wexler, M. N. (2001). The who, what and why of knowledge mapping. *Journal of Knowledge Management*, *5*(3), 249–264.

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

© 2026 The Sam Houston State University Institute for Homeland Security.

Kinney, A. (2026). Losing What We Know: Organizational Forgetting as a Pathway to Normalized Deviance in Critical Infrastructure Organizations. (Report No. 2026 - 1043). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/4J6SM

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY