Disasters are Rarely Failures of Knowledge

Primatech Inc.

September 2025

We live in a world where industrial and natural disasters continue to occur with regularity. In order to prevent these disasters, it is essential to understand and address the common factors that contribute to them. Such knowledge is critical for those charged with safeguarding lives, assets, and the environment.

While uncertainty can play a role in risk recognition, many catastrophic risks fall into the category of "known knowns" rather than unforeseen threats. Despite clear awareness, decision-makers often fail to act decisively. This inaction arises from flawed reasoning, weak risk governance, and the absence of a proactive safety culture.

These failures are especially troubling when a duty of care exists toward vulnerable groups that have a greater exposure to harm and less capacity to respond or recover. In such cases, the precautionary principle demands that protective measures be taken even when full certainty is lacking.

A "failure of imagination" occurs when people neglect to anticipate, conceptualize, or prepare for events that, although unlikely, remain entirely possible, often because they fall outside of past experience or expected patterns. It reflects an inability to envision how complex systems can fail in unexpected ways or to grasp the severity of consequences despite prior warnings and prior knowledge.

Multiple factors contribute to the failure of imagination. They are described below.

Cognitive and Psychological Factors

These are factors that shape how individuals and groups perceive, interpret, and respond to risks, often leading to dangerous underestimation or inaction. Key cognitive and psychological factors include:

Optimism bias: People believe that "bad things happen to others, not to us, or it won't happen again in our lifetime", leading them to underestimate their true vulnerability.

Overconfidence and normalcy bias: People downplay the likelihood of recurring disasters, rationalizing that "it happened before but is unlikely to happen again soon" or "it has never happened to me, so it won't now."

Probability neglect: Low-probability but severe risks are dismissed because people focus narrowly on how unlikely an event seems, rather than on its potentially catastrophic consequences.

Availability heuristic: Similar past events should keep risks salient but people judge risks based on what is most vivid or recent in memory. If a threat is abstract, hasn't occurred recently, or recent similar events were mild, people discount the risk and the need to act feels less urgent.

Recency effect: The absence of recent disasters causes threats to fade from collective memory, weakening preparedness and vigilance over time.

Historical anchoring: There is an over-reliance on past patterns and experiences to predict future events, ignoring the potential for rare or extreme scenarios.

Cognitive rigidity: Planning and decision-making are constrained by a focus on familiar, known scenarios, rather than considering novel, extreme, or cascading failures.

Psychological discomfort and inertia: Confronting the possibility of catastrophic events is uncomfortable and emotionally taxing. People tend to prefer the reassuring illusion of stability, avoiding difficult discussions or preparations that highlight vulnerability and uncertainty.

In summary, people often underestimate or ignore serious risks due to deeply rooted cognitive and psychological tendencies. Optimism bias, overconfidence, and normalcy bias lead them to believe disasters are unlikely to recur or affect them personally. Probability neglect and the availability heuristic cause individuals to focus on how unlikely a risk feels rather than on its potential severity, especially if no recent vivid examples exist (recency effect). Historical anchoring and cognitive rigidity further trap decision-makers in familiar patterns, preventing them from considering extreme or novel scenarios. Finally, psychological discomfort and inertia make it easier to avoid confronting unpleasant truths, reinforcing complacency and delaying critical preventive actions.

The 2005 Texas City refinery explosion involved multiple cognitive and psychological factors. The incident occurred during the startup of an isomerization unit and killed 15 people and injured more than 170. Over time, unsafe practices became routine (normalization of deviance - see next section), such as relying on sight glasses instead of properly working level instrumentation and allowing blowdown drums to vent to the atmosphere. Operators and managers had grown overconfident in their ability to "manage around" faulty alarms and equipment issues. There was a prevailing belief that "we've always done it this way, and nothing bad has happened," leading to a false sense of security (optimism bias). This mindset downplayed the likelihood of severe consequences despite repeated near misses. High personnel turnover and lack of consistent training contributed to a culture of complacency. Warning signs, such as previous incidents and audit findings, were ignored or deferred.

The Texas City disaster is a textbook example of how cognitive biases, normalization of deviance, and complacency can undermine safety systems and enable catastrophic failures, even when hazards are well known.

Social and Cultural Factors

These are factors that reflect collective behaviors, shared beliefs, norms, and traditions that shape how groups perceive and respond to risk. Key social and cultural factors include:

Groupthink and status quo bias: Decision makers may avoid advocating for costly safety measures to maintain harmony, avoid conflict, or because others downplay the threat. This reinforces a false sense of security and discourages dissenting voices.

Pressure for conformity: Social dynamics often discourage individuals from challenging prevailing views, leading to collective inaction even when risks are known.

Tradition and habits: Long-standing practices and cultural norms can make it difficult to introduce changes, even when those changes are clearly necessary for safety.

Economic and social inertia: Immediate economic benefits and social conveniences frequently outweigh the perceived value of risk mitigation, leading to delays or outright avoidance of preventive measures.

Normalization of deviance: Repeatedly accepting small deviations from safe practices without negative consequences gradually shifts what is considered "normal,", increasing vulnerability over time.

Complacency and erosion of safety culture: As time passes without incidents, overconfidence grows and vigilance declines. This leads to a weakened safety culture, where risks are underestimated and proactive measures are neglected.

In summary, collective behaviors and social dynamics often discourage proactive safety actions. Groupthink, conformity pressures, and long-standing traditions make it difficult to challenge established norms or advocate for necessary changes. Economic and social inertia favor short-term convenience and immediate benefits over long-term risk reduction, while normalization of deviance and complacency gradually weaken safety culture, increasing overall vulnerability.

The 1988 Piper Alpha offshore oil platform disaster in the North Sea involved social and cultural factors. A catastrophic explosion and fire destroyed the platform, resulting in 167 deaths. It involved groupthink and the status quo bias. A strong culture of production over safety dominated operations. Workers and managers focused on maintaining output targets rather than questioning unsafe practices or shutdown decisions. Concerns from workers about safety systems and maintenance issues were not actively encouraged or acted upon. Employees felt pressured to comply with established procedures and avoid disrupting operations, even when safety concerns arose. Individuals were reluctant to challenge authority or suggest stopping production. The practice of performing maintenance on key safety-critical equipment while the platform was still operating had become routine, even though it introduced serious risks (normalization of deviance). Over time, operating with partial safety systems offline was accepted as normal. There was an overreliance on the belief that existing fire and gas systems were sufficient, despite known vulnerabilities. Safety procedures and permit systems were inconsistently enforced, and audits failed to correct these cultural weaknesses.

Piper Alpha is a classic example of how social pressures, groupthink, and an ingrained culture prioritizing production over safety can override formal safety systems and directly lead to catastrophic failures.

Economic and Incentive-Related Factors

These are factors that are driven by financial motivations and cost pressures. They distort safety decisions. Key economic and incentive-related factors include:

Cost-benefit misjudgment: Decision makers often focus too heavily on immediate, visible costs of risk mitigation while underestimating or discounting the potential human, financial, and reputational losses from a disaster. This reflects a failure to internalize true risk through expected value thinking (probability X consequence).

Perceived cost barriers: The cost of risk mitigation measures feels more immediate and tangible than hypothetical future losses, making them easier to rationalize away or postpone.

Resource constraints and competing priorities: Budget pressures, competing operational needs, and politically popular projects frequently override "invisible" safety improvements or long-term safety investments. As a result, organizations hesitate to allocate resources to prepare for seemingly improbable but high-consequence events.

Short-termism: The preference for avoiding upfront costs and maximizing immediate benefits leads to under investment in prevention and resilience. Budgets and profit-driven pressures reinforce this behavior.

Prioritizing convenience over safety: Operational efficiencies or short-term conveniences are often chosen over more costly but necessary mitigation measures, reinforcing risky practices.

Moral hazard: When those responsible for risk decisions do not personally bear the full consequences of failure, they are more likely to accept higher levels of risk. They may under invest

in safety or defer critical measures, knowing that others will share or absorb the costs. This erosion of accountability weakens incentives to act cautiously and undermines proactive risk prevention.

In summary, financial pressures and misaligned incentives often lead decision-makers to prioritize short-term savings over long-term safety. Immediate costs of mitigation are overemphasized, while potential losses from disasters are underestimated or dismissed. Budget constraints, competing priorities, and a focus on operational convenience further discourage investment in prevention. Additionally, moral hazard, where decision-makers do not fully bear the consequences of their choices, weakens accountability and increases the likelihood of risky, under-protected systems.

The 2010 BP Deepwater Horizon blowout and oil spill at the Macondo well in the Gulf of Mexico involved economic and incentive-related factors. The incident led to explosions and fire that killed 11 workers, destroyed the rig, and caused the largest marine oil spill in history.

BP and its contractors were significantly behind schedule and over budget on the Macondo well. The operating cost of the rig was estimated at around $1 million per day, creating intense pressure to finish quickly. Several safety-critical decisions were made in favor of saving time and reducing costs, such as choosing a less robust well design and skipping certain cement integrity tests. Management prioritized immediate operational savings and rapid completion over long-term well integrity and environmental safety (short-termism). Decisions were framed in terms of immediate deadlines rather than potential catastrophic consequences. Installing additional devices to help ensure proper cementing and conducting additional testing were viewed as expensive and unnecessary delays. The focus on minimizing "non-productive time" led to bypassing safety checks.

Contractors and executives did not personally bear the full consequences of potential failure (Moral hazard). While they faced reputational risk, financial and environmental damages were largely externalized to the broader company, insurance, and the public.

The Deepwater Horizon disaster highlights how short-term financial pressures, cost-cutting decisions, and misaligned incentives can directly compromise safety, leading to catastrophic consequences.

Organizational and Structural Factors

These are factors that relate to how organizations and governance systems are designed to manage risk, ensure accountability, and implement safety measures effectively. Key organizational and structural factors include:

Fragmented responsibility and weak governance: When no single individual or body "owns" a risk, it easily falls through organizational cracks. This fragmentation allows blame to be shifted or diluted after an incident, undermining both accountability and prevention.

Diffusion of responsibility: When responsibilities are shared across multiple parties, each actor may assume that someone else is managing the risk. This collective ambiguity often leads to inaction and overlooked vulnerabilities.

Lack of accountability: Decision makers may not face direct consequences for failing to address known risks creating little personal incentive to prioritize safety or proactively invest in risk mitigation.

Regulatory or governance failure: Weak enforcement, unclear standards, or insufficient oversight from regulatory bodies and other authorities allow hazards to persist unchecked, even when risks are well documented.

Inadequate emergency response plans: Effective plans must account for all credible scenarios and include robust, effective, regularly-tested warning systems. Adequate means of egress and

evacuation must be established, and drills conducted to ensure readiness. Failure in any of these areas can turn a manageable hazard into a catastrophic event.

In summary, weak governance structures, fragmented responsibilities, and lack of accountability allow critical risks to slip through the cracks. When no one clearly "owns" a risk, inaction and blame-shifting become common. Insufficient regulatory oversight and inadequate emergency planning further erode preparedness, turning manageable hazards into disasters.

The 1984 Union Carbide Bhopal gas tragedy in India involved organizational and structural factors. A runaway reaction in a pesticide plant released a large cloud of methyl isocyanate (MIC) gas. Over half a million people were exposed; thousands died immediately, and many more suffered long-term health effects. Union Carbide Corporation in the US and its Indian subsidiary, UCIl, had overlapping and poorly defined lines of control. Critical decisions about safety investments and staffing were made without clear accountability between headquarters and local plant management. Local managers assumed that design and safety standards from the parent company were sufficient, while corporate leadership assumed local operations would manage day-to-day safety. This led to neglected maintenance and insufficient safety oversight. Cost-cutting was prioritized over maintenance and safety upgrades. Key safety systems, such as the refrigeration unit for MIC storage, had been shut down to save money. Senior leadership did not face direct consequences for deferring safety investments, leading to a weakened safety culture.

Indian regulatory oversight was minimal and enforcement weak. There were no rigorous inspections or effective penalties to ensure compliance with safety standards. The plant's emergency response plan was outdated, poorly communicated, and never properly tested. Local hospitals were unprepared for mass chemical exposure, and there was no effective community warning system.

The Bhopal disaster exemplifies how fragmented responsibility, weak governance, lack of accountability, poor regulatory oversight, and inadequate emergency planning together create systemic organizational failures that can turn operational hazards into mass-casualty disasters.

Historical and Learning-Related Factors

These are factors that reflect how past experiences and the lessons derived from them shape an organization's future approach to risk Key historical and learning-related factors include:

Failure to learn from previous incidents: While "lessons learned" are often formally documented after an event, they may not be fully internalized or translated into lasting change. Over time, institutional memory fades, corrective actions can lose momentum, and complacency takes hold, allowing the same vulnerabilities to persist or re-emerge.

Negligence: Unfortunately, failing to learn and act, and willful disregard of known, documented risks can sometimes play a role. When organizations or leaders consciously choose not to act on historical evidence or prior warnings, it reflects an ethical and systemic breakdown that can have tragic consequences**.**

In summary, organizations often fail to internalize lessons from past incidents, allowing complacency and repeated vulnerabilities to persist. In some cases, willful disregard of known risks reflects not just oversight but negligence, leading to preventable tragedies.

The 2011 Fukushima Daiichi nuclear power plant disaster in Japan involved historical and learning-related factors.

A massive earthquake and subsequent tsunami struck Japan, disabling power and cooling systems at the Fukushima Daiichi nuclear power plant. This led to multiple core meltdowns, hydrogen explosions, and significant radioactive releases. Prior to 2011, Japan had experienced historical tsunamis of similar or even greater magnitude. There was evidence, including centuries-old stone

markers and documented tsunami heights indicating that much larger waves than the plant design basis could occur. The 2004 Indian Ocean tsunami and earlier domestic near-miss events had highlighted vulnerabilities of critical coastal infrastructure, but these lessons were not adequately integrated into plant upgrades or emergency plans.

The plant operator, Tokyo Electric Power Company, and regulatory authorities were aware that the plant's sea wall and backup systems were inadequate to protect against a major tsunami. However, upgrades were deferred or minimized to avoid high costs and operational disruptions. Reports and internal assessments warning of potential flooding risks were downplayed or ignored. In some cases, engineers and inspectors who raised concerns faced internal resistance. Over time, complacency grew, and reliance on historical assumptions (It won't happen here again.) replaced proactive risk assessment. Organizational inertia and lack of a true safety culture eroded lessons learned from previous natural disasters.

The Fukushima Daiichi nuclear power plant disaster illustrates how failure to internalize and act on historical lessons, willful neglect of known vulnerabilities, and erosion of institutional memory can turn known risks into catastrophic events.

Disasters are rarely the result of a complete lack of knowledge. More often, they arise from a collective failure to imagine extreme but plausible scenarios and a reluctance to act decisively on well-established risks. Cognitive biases, cultural and social dynamics, economic pressures, and structural governance weaknesses all intertwine to erode vigilance and diminish proactive safety measures.

Effective risk management requires decision makers to champion long-term resilience investments, not just short-term cost savings. In high-hazard contexts, especially where a duty of care exists, decision-makers have a duty to act decisively on low-probability, high-consequence risks, even when mitigation is expensive or unpopular.

Companies can implement a multi-layered, proactive approach to address the factors described above that contribute to the failure of imagination, The approach is described below.

Strengthen Risk Awareness and Imagination

Imagination is not a luxury in risk management. It is a necessity. Many disasters stem not from lack of information, but from the inability or unwillingness to envision how known risks could evolve into catastrophic failures. To counteract this issue, companies must embed structured foresight into their processes using approaches such as:

Scenario planning and stress testing: Regularly conduct planning exercises that go beyond routine cases to include extreme, low-probability, high-impact events (so-called "black swans"). These exercises help break the illusion of control and expand the boundaries of what teams consider plausible.

Red teaming: Use independent teams to introduce healthy skepticism by challenging core assumptions, identifying blind spots, and proposing alternative failure pathways. This practice encourages intellectual humility and keeps complacency in check.

Institutionalizing "failure of imagination" lessons: Incorporate real-world disasters and near misses into training of facility personnel and planning to help dismantle normalcy bias and remind teams that the unimaginable has happened before and can happen again.

Address Cognitive and Psychological Biases

Human cognition is not naturally wired for rare, complex risks. Biases such as optimism bias ("It won't happen here"), normalcy bias ("It's never happened before"), and probability neglect ("That's too unlikely to consider") routinely undermine sound decision-making. They can be addressed using these approaches:

Bias training for leaders and key decision makers: Even the most experienced professionals are vulnerable to cognitive biases that distort risk perception and hinder proactive decision-making. Bias training is essential to help decision makers recognize and manage these unconscious tendencies before they influence high-stakes choices.

Effective bias training programs use real-world case studies, interactive simulations, and self-assessment tools to help participants identify how these biases show up in their own thinking. Training should also introduce debiasing techniques, such as structured decision-making frameworks, checklists, devil's advocacy, and red teaming, to improve analytical rigor. Importantly, bias training should not be limited to safety specialists. It must reach leaders, engineers, planners, and executives whose decisions influence risk exposure. Embedding this awareness across all levels of a company increases the likelihood that someone will catch a flawed assumption or a critical blind spot before it leads to harm. By equipping decision-makers with the tools to recognize and counteract cognitive biases, companies can foster more realistic, imaginative, and precautionary approaches to risk.

Promote a questioning culture: Companies should promote a questioning culture where concerns, dissent, and conservative (safer) viewpoints are not only tolerated but rewarded. Empowering employees to speak up is critical for identifying early warning signs of possible incidents.

Use data visualization and storytelling: One of the major challenges in process safety and risk management is that many threats are abstract, invisible, or statistically remote, making them difficult for people to internalize. Technical data alone often fails to generate the emotional engagement or urgency needed to prompt action. This is where data visualization and storytelling become powerful tools.

Data visualization helps translate complex risk assessments, monitored metrics, or historical trends into intuitive formats, such as heat maps, dashboards, animations, or failure pathway diagrams. Visuals allow teams to see patterns, identify anomalies, and grasp the scale or proximity of risks at a glance. For example, a bow tie diagram showing barriers communicates far more than a static report.

Visual tools also support scenario-based planning, allowing users to interact with different variables and see how risk levels change under various assumptions. This fosters deeper engagement and encourages imaginative thinking by making invisible hazards more concrete and understandable.

However, data alone rarely changes behavior. Storytelling bridges that gap. Real-world incident narratives, especially those involving relatable decisions or overlooked warning signs, help teams emotionally connect with the consequences of failure. Stories humanize risk, making it less theoretical and more immediate. Effective stories don't just recount what went wrong, they explore why it happened, including the social, psychological, and organizational factors involved. Stories from other industries, near misses, or "close calls" within the company can all be powerful prompts for reflection and discussion.

Combining data and storytelling, for example, overlaying timeline data on a narrative of a major accident, or animating how a failure propagated through a system, creates a compelling learning experience. It counteracts the abstract nature of risk and makes threats feel real, imaginable, and urgent.

Ultimately, using data visualization and storytelling together engages both analytical and emotional reasoning. This dual approach helps overcome biases, such as the normalcy bias and recency effect, prompting individuals and companies to take threats seriously before they escalate into disasters.

Reform social and cultural dynamics

Cultural norms shape how seriously risk is taken. When safety is viewed as an afterthought or an annual audit exercise, critical vulnerabilities go unaddressed. These issues can be addressed using these approaches:

Strengthen safety culture: A strong safety culture is not defined by posters on the wall or annual audits. It is reflected in everyday behavior, decisions, and priorities of facility personnel. To be effective, safety and risk awareness must be embedded into the fabric of daily operations, not treated as a separate or occasional activity. This means that safety considerations should be actively integrated into routine meetings, from shift handovers to executive briefings. Risk-related questions, such as "What's changed since yesterday?", "What could go wrong with this task?", or "Are we assuming too much?", should be part of the normal rhythm of work conversations, not just safety stand-downs or incident reviews.

Similarly, maintenance and engineering activities should routinely incorporate risk assessments, job safety analyses, and pre-task briefings. Personnel must be encouraged to think beyond the task at hand and consider how their actions affect overall system integrity and long-term reliability.

At the strategic level, safety and resilience should be given equal weight with production targets and cost metrics. Capital projects, staffing decisions, and organizational changes must be evaluated not only for efficiency but also for their impact on risk exposure and safety performance.

A truly embedded safety culture also empowers individuals at all levels to identify and act on potential hazards without waiting for formal permission or fearing retaliation. When people are confident that raising a concern or stopping work is seen as responsible, not disruptive, it fosters vigilance and accountability.

Leadership must model this mindset. When executives and managers consistently prioritize safety in decision-making, allocate resources for prevention, and recognize safe behaviors, not just outputs, they signal that safety is not a "nice to have," but a core organizational value.

Embedding safety and risk thinking into daily operations builds a culture where proactive identification and mitigation of hazards become second nature, turning imagination and foresight into routine tools of resilience.

Foster accountability and transparency: Sharing risk assessments, preparedness plans, and follow-up actions openly within the company and with the public builds trust and reinforces collective vigilance.

Regular drills and community engagement: Keep risk awareness active and ensure that everyone, from operators to the public, understands their role in preventing and responding to emergencies.

Realign economic and incentive structures

If financial and operational pressures outweigh safety concerns, even well-intentioned risk management can be sidelined. These issues can be addressed using these approaches:

Link executive and leadership incentives to safety and resilience metrics, not just financial or operational targets: In many companies, executive performance is measured almost exclusively by

financial or operational outcomes, such as profitability, production volume, efficiency, or shareholder returns. While these outcomes are important, when they dominate incentive structures, they can unintentionally de-prioritize safety and resilience. This imbalance creates pressure to cut corners, defer maintenance, or overlook weak signals of emerging risk in pursuit of short-term gains.

Linking executive and leadership incentives to safety and resilience metrics sends a clear message that protecting people, assets, and the environment is not a secondary concern but a strategic priority. Integrating safety performance into the same scorecards and incentive systems as financial outcomes ensures that risk management becomes a leadership priority and strengthens accountability at the highest levels.

Safety and resilience metrics and incentives can take various forms:

Incentive-based safety KPIs: For example, reductions in serious incidents, process safety events, or near-miss reporting rates (with appropriate safeguards to avoid underreporting).

Lagging and leading indicators: For example, completion of safety-critical maintenance, participation in drills, closeout of audit findings, and implementation of risk-reducing actions.

Resilience-focused metrics: For example, barrier health monitoring, scenario readiness, or effectiveness of emergency response tests.

For incentives to be credible and effective, they must be quantifiable, verifiable, and tied to meaningful outcomes, not just superficial metrics, such as total recordable injury rates, that may not reflect systemic risk. Also, leaders must be evaluated not only on performance during normal operations, but also on how well they prepare for and manage abnormal conditions. Recognizing and rewarding investments in prevention, contingency planning, and long-term risk reduction reinforces forward-looking behavior rather than reactive firefighting. These incentives also influence organizational culture. When executives are seen actively discussing safety performance, participating in drills, asking critical risk questions, and promoting proactive safety initiatives, it sets a tone of seriousness and commitment. It legitimizes safety efforts across all levels of the company and fosters a culture in which risk management is not seen as an obstacle but as an enabler for continued safe and reliable operations.

Internalize costs: Many of the most significant risks in process safety, such as aging infrastructure, deferred maintenance, climate-related hazards, and systemic vulnerabilities, are long-term in nature. However, traditional financial decision-making often discounts these risks because their consequences lie in the future or are difficult to quantify. As a result, preventive investments are delayed, and systemic weaknesses accumulate unnoticed. To correct this imbalance, companies must internalize the costs of long-term risks bringing their future financial impact into today's decision-making. This can be done by embedding risk-related costs into the financial structures and incentives that guide behavior at all levels. Insurance pricing, regulatory penalties, and liability frameworks can be used to make long-term risks financially visible today.

Insurance pricing is a powerful mechanism. When insurance premiums reflect a company's actual risk profile based on factors such as regulatory compliance, historical incidents, hazard exposures, and resilience measures, they create a direct financial incentive to invest in risk reduction. Similarly, risk-based deductibles can reward proactive mitigation and penalize negligence or inaction.

Regulatory penalties and enforcement frameworks also play a key role. Large fines for non-compliance, safety violations, or near-miss cover-ups increase the cost of risky behavior. Clear accountability for both individuals and companies helps shift the calculus toward prevention over reaction.

Liability frameworks, including civil and criminal liability for preventable accidents, further increase financial visibility. When boards, executives, and other decision makers understand that their

decisions today could carry personal or corporate consequences tomorrow, whether in the form of lawsuits, clean-up costs, or reputational damage, they are more likely to factor long-term risk into current priorities.

Companies should no longer treat safety and resilience as external to core business considerations. Instead, they should be integrated into decision-making to align short-term actions with long-term risk exposure to reflect the real costs of unsafe practices, bringing distant consequences into present decision-making. By doing so, the hidden costs of unsafe practices are made visible, and future consequences are factored into present choices.

Dedicated safety and resilience budgets: Ensure these funds are protected from short-term operational pressures. Treating these investments as essential infrastructure, not optional extras, is vital for long-term safety and resilience.

Strengthen organizational and governance frameworks

Systemic risk management requires clear ownership, strong enforcement, and cross-functional coordination. Here are some important actions to take:

Clarify roles and ownership: Clearly assign responsibility for each risk and ensure it is monitored and mitigated so that no risks fall through the cracks.

Regulatory enforcement and corporate oversight: Regulators play a critical role in maintaining process safety through independent oversight, routine inspections, and enforcement of penalties for non-compliance. Their presence helps ensure that organizations adhere to established safety standards and remain accountable for managing risk. However, regulatory enforcement alone is not sufficient.

Corporate oversight is equally important. Boards of directors, executive leadership, and corporate risk committees must take an active role in setting safety expectations, reviewing performance, and ensuring that safety remains a core business priority. This includes allocating resources, demanding transparency, and challenging assumptions, especially when trade-offs between safety and operational targets arise.

Without consistent and credible external and internal oversight, the most robust safety systems can degrade over time. Gaps in accountability, complacency, or shifting priorities can lead to the erosion of controls, normalization of deviance, and growing vulnerability. Sustained vigilance from both regulators and corporate leaders is necessary to maintain high standards and protect against preventable disasters.

Cross-functional teams and joint risk committees: Break silos that isolate safety functions from operations, engineering, and finance by creating joint risk and safety committees across departments and disciplines. Coordinated decision making enhances overall situational awareness and ensures a unified response to risks.

Ensure robust emergency response plans: While prevention is the cornerstone of process safety, no system is immune to failure. That is why robust emergency response planning is essential, serving as the last line of defense when other layers of protection fail. Emergency response plans must Include comprehensive, regularly tested warning systems and evacuation procedures.

Learn from history and act Incidents become tragedies when the same mistakes are repeated. Companies must commit to systematically learning from both internal and external incidents. Formal "lessons learned" programs should be established that document findings and ensure corrective actions are tracked, verified, and translated into practice.

Maintain institutional memory: In high-hazard industries, institutional memory, that is, the accumulated knowledge of past incidents, near misses, design rationales, and operational workarounds, etc., is critical to sustaining safety performance over time. Yet this memory is often fragile, especially in the face of retirements, turnover, organizational restructuring, and reliance on contractors. Without deliberate efforts to preserve and transfer this knowledge, companies risk repeating avoidable mistakes, especially those tied to hard-earned safety lessons. Relearning painful lessons not only undermines trust and credibility but also reflects a fundamental breakdown in risk management. To prevent this from happening, companies must systematically capture and transmit critical safety knowledge. Approaches include:

Documentation: Ensure that incident investigations, design decisions, hazard analyses, and risk assessments are clearly recorded, accessible, and regularly updated. These records should not just exist in archives, but be actively referenced in planning and operations.

Onboarding and Training: New employees, especially those in operations, engineering, and management, should be oriented not just to tasks and policies, but to the history of safety decisions, process hazards, and prior failures. Context builds caution and confidence.

Mentoring Programs: Pairing experienced personnel with newer staff members allows for informal knowledge transfer that may not be captured in documents. Veterans often carry deep insights into system vulnerabilities, cultural dynamics, and historical workarounds.

Knowledge Retention: Before key personnel retire or transition, conduct structured interviews, debriefings, or knowledge capture sessions. Use this input to strengthen procedures, training materials, and decision-making frameworks.

Digital Tools and Knowledge Management Systems: Implement centralized platforms where lessons learned and risk intelligence can be stored, retrieved, and used in real time to inform decisions.

Maintaining institutional memory is not just about preserving the past, it is about protecting the future. When lessons are embedded into systems, culture, and training, companies become safer, more adaptive, and less vulnerable to the costly cycle of rediscovery.

Practice continuous improvement: Effective process safety is not static. It must evolve alongside changing operations, technologies, and threats. Continuous improvement is essential for maintaining and strengthening safety performance across all elements of a process safety management system. Rather than treating risk assessments, procedures, training, etc. as "one and done," companies should adopt a mindset of ongoing refinement, ensuring that every element of their safety program adapts to new information, operational feedback, and lessons learned. By applying continuous improvement across all elements of process safety, companies move beyond compliance and toward true operational excellence and resilience. This approach helps prevent complacency, ensures that weak signals are acted upon, and positions the company to anticipate and adapt to future risks.

Conclusion

Addressing the failure of imagination in process safety requires more than technical fixes or procedural solutions. It calls for a fundamental cultural shift toward proactive, ethical, and imaginative risk management. Companies must cultivate the foresight to anticipate how complex systems can fail, the courage to challenge assumptions, and the discipline to take preventive action before harm occurs.

By embedding these principles across all dimensions of the enterprise, technical, behavioral, cultural, and organizational, companies can move beyond reactive compliance and build genuine resilience. When risk awareness, creativity, and accountability are woven into every level of the

company, from the front lines to the boardroom, both companies and communities become far better equipped to safeguard lives, assets, and the environment.

The risks are often visible. The challenge is having the vision to see them and the will to act upon them before it is too late.