

Insider Threats in the Water Sector

A Growing and Underestimated Risk

WRITTEN BY

Alec Davison, Gate15
David Pounder, Gate15

2026



**INSTITUTE FOR
HOMELAND SECURITY**
SAM HOUSTON STATE UNIVERSITY



Insider Threats in the Water Sector A Growing and Underestimated Risk

Alec Davison, Gate15
David Pounder, Gate15

September 2026

Table of Contents

INTRODUCTION	1
PROBLEM DISCUSSION	3
How Real is the Threat - A Numbers Game	3
Defining the Threat.....	4
Types of Insiders	5
Insider Threat Motivations	7
Manifestations of Insider Threats	8
Understanding Behavior and Employee Dissatisfaction	9
Recent Trends and Examples	10
Insider Threat Case Studies.....	14
WAY FORWARD / MITIGATIONS.....	19
CONCLUSION	24
RESOURCES	25
ABOUT THE AUTHORS	26
REFERENCES	27

INTRODUCTION

Insider threats are an enduring risk to the water and wastewater sector. In recent years, several converging factors have heightened that risk. It is not limited to malicious employees or one-off acts of sabotage. It is a broader risk created when trusted individuals have access to an organization's people, facilities, information, systems, or operations. Actions they take, whether intentional or unintentional, can result in harm to the organization, its clients, customers, people, and data. As organizations continue to rely on cloud services, remote access, third-party partners, automation, and increasingly connected operational environments, the number of users and identities given authorized access to an organization continues to grow. That access is necessary for daily operations, but it also creates risk when users make mistakes, ignore policies, are manipulated by outside actors, misuse privileges, or act on a personal grievance.

Current events underscore the scope of the challenge, especially in critical infrastructure where trusted access can quickly create operational, public health, and safety consequences. The Water Information Sharing and Analysis Center (WaterISAC), a nonprofit organization dedicated to providing security and resilience information to the water and wastewater sector, reports that insider threats are a growing concern to water and wastewater utilities. This is due to several factors, including:

- Heightened geopolitical tensions.
- Increasing Information Technology (IT) and Operational Technology (OT) convergence.
- Increased access by contractors and other third-parties to water and wastewater controls (including the use of remote access).
- Calls by various violent extremists to recruit insiders in critical infrastructure organizations.ⁱ

Indeed, reporting over the past year has noted:

- Employees and former employees (allegedly) stealing source code and proprietary documents.
- Trusted workers sabotaging systems following workplace disputes.
- Insiders misusing access for competitive advantage, and
- Critical Infrastructure personnel taking actions that could impact public safety.

Detecting insider threats in the water sector must be viewed as mission-essential, not simply an administrative or cybersecurity function. Water systems rely on a blend of

interconnected technologies: physical access, field operations, SCADA and other operational technology, chemical treatment processes, vendor support, and after-hours emergency response. This creates opportunities for insider risk. A dedicated insider risk program can help organizations aggregate data from across the environment to identify when behavior, access, or operational activity deviate from what is expected, or when there are concerning trends across the workforce. The goal is to detect these signals early enough to engage, assess, and intervene before they become larger issues.

The insider threat concern is especially acute given that current and former employees, contractors, and vendors understand the inner workings of organizations by the very nature of their access. They know facility layouts, processes, remote access pathways, security procedures, and OT, not to mention what security controls are in place and intended to reduce risk. If that access or knowledge is misused, even a single action could affect water quality, service continuity, emergency response, and public confidence. Moreover, the water sector supports virtually all other critical infrastructure that underpins normal society function. This underscores the far-reaching societal impacts an insider threat incident at a water utility can have.

Understanding insider threat risk requires a whole-of-organization approach. Effective programs should bring together cybersecurity, physical security, human resources, legal, privacy, operations, and leadership to identify concerning behaviors, protect critical assets, and determine appropriate intervention options. The intent is not to create a culture of suspicion. Rather, it is to build a culture of accountability and awareness where employees understand the risk, know how to report concerns, and trust that those concerns will be handled responsibly. Whether an organization has a mature insider threat program or is just beginning to address the issue, there are several practical steps that can reduce risk, including clear policies, least privilege, strong onboarding and offboarding practices, monitoring for anomalous behavior, bystander reporting, and a multidisciplinary process to review and respond to concerns.ⁱⁱ

This white paper examines the importance of understanding insider threat risk and developing practices that are realistic, scalable, and aligned to the organization's mission, with specific emphasis on detecting and addressing risk in critical infrastructure and the water sector. It begins by defining insider risk and the types of harm insiders can cause, then discusses behavioral, technical, and operational indicators, recent trends and case studies, and practical mitigation measures. Ultimately, organizations that are best positioned to reduce insider threat risk are those that treat it as an enterprise risk management issue—one that requires visibility, trust, governance, and coordinated action before a concern becomes an incident.

PROBLEM DISCUSSION

How Real is the Threat - A Numbers Game

How real is the threat? Consider the following from SentinelOne (May 6,2026):

- The annual cost of insider incidents is approximately 19.5 million USD per organization in 2026.
- About 55% to 56% of incidents can be traced back to negligence.
- Contractors and business partners account for 15% to 25% of insider threats worldwide.
- Companies who implement mature insider programs can prevent up to an average of 7 incidents per year and avoid losses of up to 8.2 million USD annually.
- Public administration and education experience fewer deliberate insider attacks but more non-malicious error. Misaddressed files, misconfigured sharing, and mishandled records repeatedly show up in 2026 insider threat statistics outlook summaries across government and academic records.
- Credential abuse and misuse of privileged access feature in roughly 22% of recent breach investigations as the initial access vector.
- Analysts found that breaches tied to malicious insiders with elevated privileges cost on average around \$4.9 million USD per event, among the most expensive scenarios tracked.ⁱⁱⁱ

The above numbers don't fully capture the next evolution of the risk. A 2026 report from Proofpoint notes that, while 87% of organizations leverage Artificial Intelligence (AI) beyond piloting it, only 63% have controls in place to manage it.^{iv} The rapid adoption of AI can increase insider threat exposure. Automated tools and agents, especially those without proper governance and controls, will have faster ways to access, summarize, move, manipulate, or expose sensitive information and operational data. In critical infrastructure environments, that means insider risk is not only about who has access, but also about how quickly that access can be amplified, automated, and acted upon before the organization detects it.

Defining the Threat

Within the water and wastewater sector, insider threats have led to significant financial losses, operational impacts (such as disruptions to the water treatment process), other negative outcomes and, in some cases, loss of life. Therefore, the key to understanding and mitigating insider threat risk is to first have a shared understanding of how insider threat risk is defined. Contrary to external threats, insider threat risk is the risk from those that the organization has already given access to, thereby assigning trust to that individual. That trust needs to be verified and is a key reason why managing insider threat risk begins at the talent acquisition process and carries through the employee lifecycle all the way through termination.

WaterISAC's 12 Cybersecurity Fundamentals for Water and Wastewater Utilities further emphasizes this point, noting that "Strong protective cybersecurity controls and system architecture can quickly be defeated by an adversary with physical or privileged access. It is common to believe our greatest threat is external and remote. However, an insider, whether an employee, visitor, vendor, contractor, integrator, or other trusted consultant can cause as much or more damage than an external threat actor."^v

Definitions

- The Cybersecurity and Infrastructure Security Agency's (CISA) Insider Threat Mitigation Guide defines an insider as: "any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems."^{vi}
- Thus, an insider threat is the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, facilities, and associated resources.

CISA further defines insider threats as:

- **A person the organization trusts**, including employees, organization members, and those to whom the organization has provided sensitive information and access.
- **A person given a badge or network access device** identifying them as someone with regular or continuous access. Can be a full-time employee, contractor, or even third-party vendor.

- A **person who develops the organization's products and services**, including those who know the secrets of the products that provide value to the organization.
- A person who is knowledgeable about the organization's fundamentals, including pricing, costs, and its strengths and weaknesses.
- A **person who is knowledgeable about the organization's business strategy and goals** and is entrusted with future plans and the means to sustain the organization and provide for the welfare of its people.
- For government functions, they can be **those with access to protected information**, which, if compromised, could cause damage to national security and public safety.^{vii}

In simple terms, insider threat risk is the danger that a trusted individual with authorized access to an organization's facilities, systems, information, or operations can misuse that access, or fail to protect it, in a way that causes harm, whether intentionally or unintentionally.

Types of Insiders

The Insider Threat definition captures unintentional and intentional threats. As noted in the data above, unintentional threats are more common and regardless of the intent of the individual, they still present risk that is driven by an insider. Their mistakes, while not malicious in nature, can still create financial impacts, reputational impacts, and even regulatory or legal impacts. Understanding the various types is essential to developing a whole-of-organization approach and the scope of the insider threat risk program.

Unintentional Threats

- **Negligence.** Exposes an organization to a threat through carelessness; these individuals put the company at risk by ignoring policies.
- **Accidental.** Mistakenly causes an unintended risk to an organization.

Intentional Threats (Malicious). Intentional threats are actions taken to harm an organization for personal benefit or to act on a personal grievance.

Collusive Threats. A subset of malicious insider threats where one or more insiders collaborate with an external threat actor to compromise an organization.

Third-Party Threats. Threats that are contractors or vendors who are not formal members of an organization, but who have been granted some level of access to facilities, systems, networks, or people to complete their work.

Another way to look at insider types was outlined in research conducted by Elina Elveborg Lindskog, Anna Lioufas and Anna Wagman Kåring, titled, “Spies Among Us: Espionage in Europe. A study on convicted spies in Europe 2008–2024.”^{viii} While the focus of this study was on national security incidents, the concept remains applicable to the water sector and other industries. The primary difference is the motivation and the nature of the target in the incident. Their analysis looked at the malicious incidents and identified ten types which could provide a more complete representation of the risks posed by insiders. Understanding these types will also help organizations develop more focused strategies to address the risk. For example, an observer may not have direct access to information or controls but could provide insight that could allow another to take advantage of their insight.

1. **The Traditional Insider.** Someone inside an organization with access to sensitive, classified, company, or personal data. Example: an employee copies restricted files to share externally.
2. **The Ideologist.** Someone driven by political ideology, nationalism, loyalty to a country, or a belief system. Example: a worker leaks information to support a political cause.
3. **The Observer.** Someone who monitors surroundings, reports useful information, or identifies potential insiders with direct access. Example: a contractor notes security routines and reports them to another party.
4. **The Disposable.** A low-value recruit used for one-off tasks, sometimes without knowing the act's purpose. Example: a temporary worker delivers a package without knowing it supports espionage.
5. **The Intermediary.** A facilitator who handles logistics or support between a threat group and an insider. Example: a contact arranges payments or meetings between parties.
6. **The Multi-Criminal.** Someone involved in espionage as well as crimes such as sabotage, propaganda, or influence operations. Example: a person steals data while also spreading false narratives online.
7. **The Specialist.** Someone whose skills or role could expose data or proprietary information. Example: an engineer shares technical designs from a restricted project.

8. **The Mobile Spy.** Someone with routine global mobility, such as frequent travel for sales, conferences, or meetings. Example: a frequent traveler carries sensitive information across borders.
9. **The Connected Agent.** Someone recruited through cultural, family, religious, historical, or community ties to a threat actor. Example: a community contact is pressured to pass along workplace information.
10. **Espionage Rings.** Networks of operatives collaborating to conduct coordinated activities. Example: several people divide roles for collection, transfer, and support in furtherance of external threat actor's malicious objectives.

Insider Threat Motivations

Individuals involved in insider threat incidents have varied motivations, but they can be effectively grouped into four main categories – Money, Ideology, Crime or Coercion, and Ego, or better known as MICE.

Money

The insider may have financial concerns, such as having large amounts of debt, or they could have a family member that needs a medical procedure but does not have savings or insurance to cover it. It could also involve individuals who have a lavish lifestyle or spend beyond their current means.

Ideology

These are individuals who are motivated by a strong belief system. It could be rooted in their upbringing and passed down from familial ties. It could be rooted in a political cause, or inspired by religious beliefs, or loyalty to a nation-state. Another aspect is that an individual could be in opposition to their organization's mission or realize that the business's profit motivations may run in contrast to their core beliefs.

Crime or Coercion

In some cases, individuals may not always be willing participants, but they get put in a position where they may be threatened, coerced, or manipulated into helping a threat actor. In some examples, individuals who have families in parts of the world may be threatened with harm or lack of support if the individual does not do what the threat actor wants. In other instances, an individual may have made a mistake or violated a law and a threat actor, such as a foreign intelligence service, uses that as leverage to force the individual to carry out malicious activity under the threat of being reported to law enforcement.

Ego

This motivation can span several areas. An individual may feel overlooked, underappreciated, disrespected, or unfairly treated by the organization, their leadership, or their peers. Over time, this resentment can lead them to justify harmful actions as a means of proving their value, regaining a sense of control, or retaliating against people they believe wronged them. These insiders may also be motivated by a desire for recognition, status, or validation, especially if they believe they are smarter, more capable, or more deserving than others. For example, an employee who feels passed over for a promotion may take or disclose sensitive information to embarrass the organization, prove their importance, or show that the company underestimated them. The Robert Hanssen spy case was an example of an ego-driven insider.^{ix}

Manifestations of Insider Threats

Insider threats within an organization can manifest themselves in a variety of ways. Of course, insider threats of any type can lead to negative outcomes for an organization. Still, some acts are more severe than others. These acts typically include, but are not limited to violence, espionage, sabotage, theft, and unintentional acts.^x These manifestations are further defined below:

- **Workplace/organizational violence** is any action or threat of physical violence, harassment, sexual harassment, intimidation, bullying, offensive jokes, or other threatening behavior by a co-worker or associate that occurs in a person's place of employment or while a person is working.
- **Espionage** is the covert or illicit practice of spying on a foreign government, organization, entity, or person to obtain confidential information for military, political, strategic, or financial advantage.
 - **Economic Espionage** is the covert practice of obtaining trade secrets from a foreign nation (e.g., all forms and types of financial, business, scientific, technical, economic, or engineering information and methods, techniques, processes, procedures, programs, or codes for manufacturing).
 - **Government Espionage** is covert intelligence-gathering activities by one government against another to obtain political or military advantage. It can also include government(s) spying on corporate entities such as

aeronautics firms, consulting firms, think tanks, or munition companies. Government espionage is also referred to as intelligence gathering.

- **Sabotage.** Sabotage describes deliberate actions to harm an organization's physical or cyber infrastructure, including noncompliance with maintenance or IT procedures, contaminating clean spaces, physically damaging facilities, or deleting code to prevent regular operations.
 - Citibank example: An employee sabotaged the bank's computer system.^{xi}
- **Internal fraud** is the act of using access to take or inappropriately use a person's, business', or organization's money or property with the intent to benefit from it.
- **Intellectual Property Theft** is the theft or robbery of an individual's or organization's ideas, inventions, or creative expressions, including trade secrets and proprietary products, even if the concepts or items being stolen originated from the thief.
- **Unintentional Threats**, as mentioned above, can be accidents or inadvertent exposure of an organization's information, technology, etc. that causes unintended harm to an organization. This can include falling for phishing emails, downloading malicious software, or making operational mistakes that can result in loss of data or proprietary information.

Understanding Behavior and Employee Dissatisfaction

It is important to understand employee behavior, as rarely do employees randomly decide to commit harmful acts. These usually arise over time and through a series of events or incidents in employees' own lives, both within and outside of the workplace. This is why it is important that organizations have an effective insider threat risk program in place that accounts for the entire employee lifecycle - from the time they apply for a role through their termination.

Disgruntled employees rarely mask all warning signs of potential violence before carrying out an attack. Instead, many potential attackers exhibit red flags or proximal warning behaviors that together form patterns of risk, which other employees can detect and report to help prevent an act of violence before it occurs. A VOA report, for instance, found that nearly all workplace shooters showed signs of crisis (75%), or a marked change in behavior, often triggered by a job dismissal.^{xii} These indicators included failing

to comply with directives, exaggerated emotional responses, and increased interest in violence or weapons.

One way to address the complexity of insider threats is to adopt a critical pathway approach which was developed by Dr. Eric Shaw and widely adopted by other security groups and teams. This is a structured, proactive framework that maps the behavioral, technical, and organizational indicators leading to insider incidents. In practice, it outlines a sequence of events, decisions, and behaviors that typically precede an insider threat incident to create a predictive model that could be used to prevent risk. The foundation relies on understanding the why, how, and when of insider behavior.

Understanding predisposition means looking at the personal vulnerabilities, stressors, and circumstances that may make an individual more susceptible to moving toward harmful behavior. In the Critical Pathway model, the risk to the organization is typically not spontaneous; it often develops over time through grievance, ideation, planning, preparation, probing, and action. A predisposition does not mean someone will become violent or act as an insider threat, but it can help explain why a person may be more likely to interpret setbacks, conflicts, or pressures as personal injustices. Factors such as unresolved grievances, financial strain, isolation, identity conflict, resentment, coercion, or a strong need for recognition can create conditions where the person becomes more receptive to harmful ideas, outside influence, or self-justification. The goal is not to label someone as dangerous, but to recognize concerning patterns early, understand what may be driving the behavior, and intervene before the person progresses further along the pathway.

Grievances or stressors lead to behaviors to potential workplace manifestations, i.e., violations, all leading to the incident. Having mechanisms in place to monitor and alert on these areas will drive early engagement and intervention, which can ultimately help disrupt the incident before a negative outcome occurs.

Recent Trends and Examples

This section examines five of the most common manifestations of insider threat activity currently shaping risk profiles in water and wastewater utilities:

1. Unintentional insider threats
2. Employee theft

3. Cyber-enabled acts
4. Sabotage from disgruntled employees seeking retribution
5. Workplace violence.

Following the discussion of recent trends, case studies are presented for each category to illustrate how insider threats have manifested in operational environments.

Trends

The threat landscape facing the water and wastewater sector is increasingly dynamic, with a widening range of internal and external actors seeking to target the sector. In particular, insider threats are evolving and exposing new system vulnerabilities, which in turn raise the operational risk to water and wastewater utilities.

This evolution largely results from the increasing integration of digital technologies, remote access capabilities, and interconnected industrial control systems. All these can make access easier for malicious insiders. Notably, one significant cybersecurity problem facing the water and wastewater sector is the convergence of IT and OT networks. According to the WaterISAC – EPA Q1 2026 National Security Information Sharing Bulletin, this increase of connected devices has left unsecured, internet-facing critical infrastructure vulnerable to remote exploitation and allowed malicious insiders to exploit their privileged access. Malicious insiders, and other threat actors, have exploited this expanded attack surface, often targeting weak, outdated systems to disrupt water supplies or cause panic.^{xiii}

In addition to IT/OT convergence and the integration of digital technologies at critical infrastructure entities, growing geopolitical tensions and the increasing use of third parties have almost certainly led to a rise in insider threat incidents. Heightened geopolitical tensions have led to greater targeting of critical infrastructure employees by hostile foreign intelligence services who seek access to sensitive information (see below for specific examples). Relatedly, cyber-criminal groups, who are often tacitly aligned with a hostile nation state, are increasingly attempting to recruit insiders at target organizations to aid in their criminal activity.^{xiv}

The growing number of third parties involved in water and wastewater utility operations is also very likely heightening insider threat risk. According to Whistic's 2024 Third-Party Risk Management Impact Report, half of companies now work with more than 100 vendors, up from 38% in 2023. The Cyentia Institute adds that for each third-party vendor, organizations typically have indirect relationships with nearly 14 times as many fourth and fifth parties.^{xv} These figures show how much the third-party ecosystem is

expanding: each new supplier brings a web of unseen connections, and any one of them can give an attacker a way in or give an insider access to sensitive systems.

Malicious insiders represent a particularly acute concern for the water and wastewater sector due to their unique knowledge and ability to cause significant operational disruptions and public health impacts.

Recent incidents across the sector reveal that insider threats range along a spectrum of intent and impact, from inadvertent errors made by well-meaning employees to deliberate, malicious acts carried out for purposes of financial gain, revenge, or ideological satisfaction.

Furthermore, the Ponemon Institute's 2025 Cost of Insider Risks Global Report shows that insider threat risk is rising.^{xvi} Across multiple industries, documented incidents grew from 3,269 in the 2018 report to 7,868 in the 2025 study. Notably, among potential insider threats, Mimecast's 2026 State of Human Risk Report, found that 42% of organizations surveyed reported an increase in malicious insider incidents over the past year.^{xvii}

In short, insider threat incidents are rising across the public and private sectors, and malicious insider incidents, typically the most damaging kind, are expanding as well. This trend reinforces the need for a robust insider threat mitigation program.

Unintentional Insider Threats

The Ponemon Institute report found that 55% of insider threat incidents were caused by careless or negligent employees.^{xviii} This indicates that unintentional insiders remain the most frequent type of insider threat at water and wastewater utilities.

Third-Party Insider Threats

Third-Party threats arise when trusted, authorized third parties, such as maintenance contractors, software providers, system integrators, and administrative companies, misuse their access, either maliciously or unintentionally. WaterISAC and EPA's Q2 2026 National Security Information Sharing Bulletin states that "third-party vendor insider threats are a critical vulnerability for the sector."^{xix}

Utilities can also be impacted indirectly by third-party insider threats when their vendors experience cyber-attacks and other breaches. For example, in February 2026, a third-party payment processor, BridgePay, was the victim of a ransomware attack that disrupted utility billing and online payment services for municipalities and utilities in several states.^{xx}

According to the Q2 2026 National Security Information Sharing Bulletin, another type of third-party insider threat in the sector includes janitorial staff. They have physical access to facilities, control rooms, and in some cases, insecurely placed computers or network jacks.^{xxi} All create opportunities for both accidental and malicious harm. This vulnerability significantly increases when the janitorial staff work after hours and regular staff are not present to supervise or escort them.

Malicious Insider Threats

According to Verizon's Data Breach Investigations Report 2023, malicious insiders, employees and third-party contractors are most often motivated by financial gain.^{xxii} Therefore, malicious insider threat incidents at water and wastewater utilities typically manifest as employee/third-party theft or embezzlement.

Domestic threats

Malicious insider incidents not related to theft are a growing concern in the water sector and in the critical infrastructure workforce writ large. They may be disgruntled employees, those coerced by an external actor, or motivated by some sort of psychological trigger.

For example, the 2023 Verizon report found that malicious insiders are also motivated by revenge and espionage.^{xxiii} According to past Department of Justice (DOJ) indictments, in recent years, malicious insiders motivated by retribution have endangered drinking water supplies by exploiting their privileged access. This allowed them to disable water treatment system safeguards and disinfection processes.

Foreign Threats

Hostile nation states – specifically China, Russia, Iran and North Korea – are increasingly seeking to recruit insiders across every critical infrastructure sector to gain an edge over the U.S. and its allies. For instance, a recent U.S. government report warned that Chinese intelligence operatives are using an increasingly wide array of professional networking sites and online job platforms to target individuals for recruitment.^{xxiv} China seeks to obtain privileged military, political and economic information that can provide Beijing with a strategic and tactical advantage over Western nations.

Highlighting this threat, in August 2024, a man from Florida, who worked at a telecommunications firm and Information Technology company, pleaded guilty in federal court for conspiring to act as an agent of the People's Republic of China (PRC) for more than a decade.^{xxv} Court records revealed the individual obtained a wide variety of information at the request of the PRC's Ministry of State Security, including information

about the companies he worked at, Chinese dissidents, and pro-democracy advocates, among other topics. In another incident, in April 2025, a former Federal Aviation Administration (FAA) contractor pleaded guilty to acting as an agent for the Iranian government and sharing sensitive information about the aviation sector and the U.S. solar energy industry with Iranian intelligence officers.^{xxvi}

Moreover, in recent years, North Korean IT workers have used fabricated identities to infiltrate U.S. companies through legitimate job postings. Threat actors tied directly and indirectly to North Korea have run this campaign to generate revenue and steal intellectual property and data from companies worldwide, across all industries.

According to a Cross-Sector ISAC report, WaterISAC has tracked remote IT workers suspected of working on behalf of North Korea who applied for jobs at North American electric utilities.^{xxvii} In past cases, the applicants targeted remote, technology-focused positions. Because these workers have sought employment at electric utilities, they are likely to pursue fraudulent jobs at water and wastewater utilities as well. Indeed, in 2022, it was estimated that thousands of workers had been dispatched and had already penetrated many organizations.^{xxviii}

Insider Threat Case Studies

To help us better understand these trends, a series of case studies are presented below that highlight several categories of insider threat incidents at water and wastewater utilities.

Unintentional

Davis, Oklahoma: An example of an unintentional insider threat occurred in late 2024 at a small, combined (water and wastewater) utility. During the incident, the utility experienced a spike in chlorine levels after an employee error, which led to significant operational disruptions. The utility became aware of the incident after its customers reported an unusual smell and taste of chlorine in their tap water.

The utility determined that an inexperienced employee had mistakenly turned off a chlorine level monitor during a routine procedure but failed to turn it back on, resulting in chlorine levels three times higher than normal pumped into the utility's water system for 12 hours.

As a result of the incident, utility workers spent several weeks bleeding dead-end lines to reduce the amount of chlorine circulating in the system. They also partially drained a couple of the utility's water towers and, "refilled those with what we would consider our normal chlorine counts," the utility officials added. Fortunately, chlorine levels never surpassed the state required threshold, the utility got chlorine levels down to normal levels, and no public health impact occurred.^{xxix}

In another incident, a large drinking water utility experienced a hazmat incident at its treatment plant due to an unintentional error from a third-party vendor. The vendor mistakenly offloaded a chemical into the wrong tank, which led to an alarm about a possible hazmat situation. An evacuation order was issued for many hours as firefighters and first responders evaluated the situation and took appropriate actions to render the area safe.^{xxx}

Malicious

Following are examples of malicious insider threats in both the cyber and physical domains:

Financially Motivated

As noted above, among malicious insiders, water and wastewater utilities typically experience insider threats incidents from employees and third parties motivated by financial gain. For instance, an employee at a very large wastewater utility in New York was arrested and charged in October 2024 for stealing around \$14,000 in copper wire from the utility on multiple occasions. Utility employees called local scrap dealers after they discovered copper had been stolen and eventually determined the employee was responsible for the thefts. The thefts were also captured on surveillance cameras.^{xxxi}

At a medium combined utility, several utility employees were indicted for a multi-million-dollar fraud scheme. According to a U.S. Department of Justice press release, two people involved in the scheme pleaded guilty and are waiting for sentencing. The press release said that in total, seven individuals were indicted for defrauding the utility of at least \$2.4 million through a "false and fraudulent contractor scheme" between 2018 and 2022. The criminal scheme allegedly involved the creation of a fictitious business and false invoices to justify unlawful payments to charged individuals. Several utility employees allegedly falsified payment authorizations and received kick-back payments and other benefits. Officials said the seven people used coded messages to talk and destroyed evidence to avoid detection. It was also revealed in the indictment that several of the individuals had committed tax fraud in an attempt to conceal their crimes and avoid paying taxes. As of this writing, the case remains ongoing.^{xxxii}

Lastly, a small drinking water utility hired a financial firm to handle administrative tasks such as collecting payments, maintaining financial records, depositing money and providing financial reports to the utility. According to a civil lawsuit, the small third-party company, operated by a mother and son, allegedly created false financial statements, wrote unauthorized checks, and stole more than \$680,000 from the utility company.^{xxxiii}

Malicious / Revenge

Ellsworth, Kansas: On March 27, 2019, the remote log in system at the Ellsworth water treatment plant was used to shut down the plant and turn off one of its filters. a Kansas man pleaded guilty to tampering with the computer system at a drinking water treatment facility in Ellsworth County. The man, a utility employee, pleaded guilty to one count of tampering with a public water system and one count of reckless damage to a protected computer system during unauthorized access. According to court documents, the Post Rock Rural Water District hired the employee in January 2018, and his duties included monitoring the plant after hours using a remote login system. He resigned his position in January 2019. Investigators established the employee's cell phone was used to perpetrate the intrusion, and that the phone was in his possession at the time of the shutdown. He told investigators he was intoxicated and didn't remember anything about the night of March 27, 2019.^{xxxiv}

Discovery Bay, California: Another notable cyber incident involved a former employee of a private Massachusetts-based company who contracted with the town of Discovery Bay, California to operate the town's wastewater treatment facility. Prior to resigning, the employee installed software on his personal computer and the company's internal network that allowed him to gain remote access into the water treatment facility's computer network. The employee was responsible for maintaining the instrumentation and the computer systems used to control the electromechanical processes of the facility in Discovery Bay.

After the employee departed the company in 2021, he accessed the facility's computer system remotely and transmitted a command to uninstall software in the main hub of the facility's computer network that protected the entire water treatment system, including water pressure, filtration, and chemical levels. The employee was charged by the DOJ for accessing Discovery Bay's computer network and shutting it down. He spent 6 months in home confinement, followed by 36 months of probation, had to forfeit his computer and paid \$44,250 in restitution. The employee's actions were deemed deliberate and intended to cause operational disruptions, posing a possible risk to the health and safety of the community's water supply. While it was not confirmed that the

attack was revenge-motivated, the attack fit that profile in that it occurred after the employee left and no ransom demand was made.^{xxxv}

Lancaster County Township, PA: In February of 2025, a former disgruntled utility employee was arrested for allegedly making a bomb threat at the utility and for threatening to poison the utility's water supply. The disgruntled employee's threats of violence caused significant operational disruptions to the utility. Prior to the incident, the employee had been terminated. The former employee reportedly called in a bomb threat at the utility's water treatment plant and said he was going to "kill everyone," which caused an evacuation of the facility until K9 officers could clear the building. He also sent several threatening messages to employees in another administration building. That building was put under lockdown out of safety for employees since the alleged perpetrator was a former employee and knew the facility.

In a voicemail, the former employee also threatened to "poison the water supply." According to media reports, the employee made multiple calls to other utility employees threatening acts of violence and using obscene language. The perpetrator reportedly made 44 unwanted calls to just one utility employee. Following the threats of violence, police were able to identify the former employee and subsequently arrest him. The former employee was fired before the incident and was likely seeking retribution. At the time of this writing, the court case remains ongoing.^{xxxvi}

Stoughton, Massachusetts: At a large, combined utility, a disgruntled water utility employee was arrested in 2024 after he tampered with the utility's drinking water supply and made false statements to federal investigators.^{xxxvii} According to the DOJ, the former employee was accused of visiting a pumping station and disabling the chlorination system used to disinfect the drinking water. The town manager told local news outlets that an alarm would normally be sent through the station's remote monitoring system to the utility's operational headquarters and to an on-call employee's cellphone to alert them that the chlorine levels had fallen below a certain level. However, the alarm was also disabled, he said. The next morning, utility employees saw the chlorine pump had been shut off the previous evening and immediately restarted the chlorine pump. Fortunately, the utility responded in time to prevent chlorine levels from remaining low long enough to jeopardize water quality." After testing the water quality, it was determined that no additional action was necessary.

The town manager said afterwards it became apparent to utility employees the event was caused by "someone on the inside." The entrance to the pumping station is blocked by a locked gate, a chain link fence surrounds the station's building, and the door to the

building itself is made of reinforced metal, but there were no signs of forced entry, the town manager said. Every employee “involved in water treatment functions had keys to this facility. Only someone with access to and knowledge of the alarm and chlorine systems could have adjusted them in this manner.” The utility referred the matter to the local police department and the FBI. After an investigation, an employee who was not on duty or on call changed his story and admitted he adjusted the chlorine settings. The employee was placed on paid leave and eventually fired in August 2023. Notably, the town manager told local news that the former employee was unhappy about being disciplined at work and having his company truck taken away from him. “He was disgruntled. We knew he was disgruntled,” the official told local news.^{xxxviii}

Virginia Beach, Virginia: In the worst-case insider attack scenario, in May 2019, an active shooter incident claimed the lives of 12 utility workers.^{xxxix} The attack was perpetrated by a utility employee who had resigned earlier that day. The shooter was subsequently killed during a confrontation with police, following his attack. An investigation by the FBI found that the employee was motivated by perceived workplace grievances he had fixated on for years.^{xl} The assessment also determined the grievances began taking shape as early as 2014 and that the shooter purposely isolated himself and disengaged from relationships to conceal his intentions. For this reason, no individual or group was able to observe the behaviors that may have served as a warning. The FBI also assessed the shooter suffered from significant mental health stressors that appear to have contributed to the situation.

WAY FORWARD / MITIGATIONS

Water and wastewater utilities can significantly mitigate the risk of insider threats by implementing a layered insider threat program that combines:

- Physical security
- Access management
- Personnel oversight
- Continuous monitoring.

In fact, 65% of organizations with insider threat mitigation programs said those programs helped them spot risky behavior before a breach or negative employee outcome occurred, according to the report from SentinelOne.^{xli} Consistent with guidance from CISA, utilities should apply the principles of least privilege and need-to-know access for contractors, vendors, and other third parties, ensuring individuals only have access to the systems, facilities, and operational areas required for their specific work.

Utilities should also conduct background screenings, require cybersecurity and security awareness training, monitor contractor activity in sensitive areas, and regularly review physical and digital access permissions to prevent unnecessary or lingering access. Because insider threats involve individuals with authorized access and operational knowledge, utilities should establish cross-functional reporting and monitoring processes that help identify concerning behaviors, unusual access patterns, or policy violations before they escalate into operational disruptions or security incidents

The Seventh Edition of the Common Sense Guide to Mitigating Insider Threats advises organizations to adopt policies, procedures, and practices that address insider threats and reduce insider risk.^{xlii} While not every organization has the resources to build a formal insider risk management program (IRMP), taking some foundational steps remains essential. Building a security-conscious culture across all levels of the organization goes a long way toward deterring and preventing insider threats—but culture alone isn't sufficient. Organizations also need controls that go beyond awareness training to effectively prevent, detect, and respond to insider threats of every kind.

Key opportunities for organizations are listed below:

- **Establish a scalable insider threat program.** CISA recommends that organizations define the threat, detect and identify concerning activity, assess potential risk, and manage the threat through coordinated mitigation.^{xliii} This

program should serve to aggregate data from across the enterprise to identify where concentrations of risk are occurring and to identify emerging risk areas. Equally important related to insider threat identification is to:

- Identify critical assets and systems
- Define reporting thresholds
- Establish clear paths for reporting concerns and escalation.

While a dedicated program office is not required, organizations should designate clear ownership for activities and aggregate data and information related to insider risk and ensure it is appropriately reported and tracked by leadership and risk programs.

- **Create a multidisciplinary threat management process.** Insider threat mitigation should not sit with security alone; it requires a whole-of-organization approach. Whether there is a dedicated Insider Threat organization or not, that Program will rely on the entire organization to effectively identify and mitigate the risk. Organizations are encouraged to establish a small, trusted group that includes security, cybersecurity, human resources, legal, privacy, operations, and leadership representation as appropriate. This group should be responsible for reviewing reports, protecting employee privacy and civil liberties, coordinating response actions, and ensuring concerns are addressed consistently and lawfully.
- **Train the workforce and normalize responsible reporting.** Employees are often the first to observe changes in behavior, policy violations, or suspicious activity. This makes them the first line of defense, and they can provide valuable context to potential risk areas. Employee education and awareness are critical to identifying and recognizing this risk.
 - Organizations should provide recurring awareness training on insider threat indicators, acceptable use, data handling, reporting options, and the difference between reporting a concern and making an accusation. Training should also reinforce bystander reporting and make clear that reports will be handled discreetly, objectively, and without retaliation.
 - Equally important in this is to establish a clear, and transparent, reporting process. There should be clear communications on what to report and where to report. The organization should ensure they have a team that is able to intake each report, conduct appropriate analysis to assess the report, and then investigate or refer elsewhere, such as Employee Relations.

- **Strengthen access controls and lifecycle management.** Apply least privilege, role-based access, multi-factor authentication, and periodic access reviews to ensure users only have the access needed for their duties. Onboarding, job changes, leave, termination, and contractor offboarding should trigger timely access updates, return of assets, and disabling or removal of accounts. Extra attention should be given to privileged users, access to sensitive repositories or locations, removable media, and access to critical business systems.
- **Use monitoring, auditing, and documented response playbooks.** Organizations should monitor for anomalous activity such as unusual data transfers, unauthorized cloud storage use, attempts to install remote access tools, excessive printing, abnormal access to sensitive files, or access outside normal work patterns. Where appropriate, user and entity behavior analytics, data loss prevention, digital rights management, and audit logging can support early detection. Response procedures should define who reviews alerts, how information is validated, when HR or legal are engaged, and when law enforcement or other external partners may be contacted.

WaterISAC's 12 Cybersecurity Fundamentals for Water and Wastewater Utilities recommends that water and wastewater utilities consider establishing a committee of relevant stakeholders to begin evaluating viable methods to prevent, detect, and respond to insider threats.^{xliv} The committee should have representation from key departments across the organization such as human resources, legal, information technology, cybersecurity, physical security, and communications. Relatedly, in the aftermath of the shooting incident in Virginia Beach, a security risk management firm recommended the utility establish a formal behavioral threat assessment capability or an interdisciplinary Threat Assessment Team (TAT) that would help to identify and prevent workplace violence and other insider threat incidents.^{xlv}

In addition, specifically for Texas-based water and wastewater utilities, the Texas Cyber Command offers several free tools and services to help organizations enhance their cybersecurity and can also be leveraged to strengthen insider threat mitigation. The purpose of the Texas Cyber Command is to help critical infrastructure entities prepare for cyber-attacks through exercises and pre-attack coordination, defend against and mitigate attacks when they occur, and provide subject matter expertise and forensic analysis for post-attack investigations and recovery. Most recently, Project Watershed 250, launched on August 31, is a six-month pilot program that will offer free red teaming,

vulnerability assessments, system hardening, and other private sector tools to Texas water and wastewater utilities.^{xlvi}

Another important resource water and wastewater utilities can leverage is WaterISAC's Insider Threat Management – Fact Sheet. This fact sheet was developed by WaterISAC's Physical Security and Resilience Advisory Committee, to help water and wastewater utilities strengthen their insider threat management policies. It includes a series of best practices organized into five thematic sections developed by utility security professionals.^{xlvii} These five sections include:

- **Program Culture & Governance:** Focuses on strategic alignment, leadership, and organizational values.
- **Access & Privilege Management:** Covers how to control and minimize exposure to sensitive data and systems.
- **Detection & Monitoring:** Addresses proactive identification of suspicious or harmful behavior.
- **Risk Assessment & Prevention:** Focuses on understanding and reducing vulnerabilities.
- **Integrated Response & Reporting:** Prepares the organization to handle insider threats when they occur.

Finally, an important training opportunity is “National Insider Threat Awareness Month,” which occurs annually in September.^{xlviii} National Insider Threat Awareness Month provides a timely opportunity for organizations to evaluate the maturity of their insider threat programs, reinforce a culture of shared responsibility, and establish a clear roadmap for continued improvement. It also creates a natural platform to increase employee education and awareness by translating insider threat risk into practical, everyday behaviors. Organizations can strengthen engagement through several easy-to-implement activities listed below:

1. Host a “fireside chat” with senior leaders to discuss insider threat risk, explain why the program matters, and highlight the specific actions leaders take to support the mission, protect the workforce, and reinforce employee awareness.
2. Equip managers with a short discussion guide they can use during team meetings, town halls, or one-on-one conversations to help employees recognize potential indicators, understand reporting pathways, and feel comfortable raising concerns early.

3. Develop an organization-wide webinar that explains insider threat risk in plain language and focuses on the everyday actions employees can take to identify, prevent, and mitigate potential concerns.
4. Launch a short awareness campaign using intranet posts, digital signage, email tips, and quick-reference materials that reinforce key messages throughout the month and make reporting resources easy to find.
5. Create scenario-based microlearning or tabletop exercises that allow employees practice recognizing concerning behaviors, respond appropriately, and understand how early reporting helps protect both people and the organization.

In short, implementing a formal insider threat management program is a foundational security measure for water and wastewater utilities. A formal program gives utilities a structured way to set clear policies, monitor user behavior, and respond quickly to suspicious activity. Beyond protecting critical systems from misuse, these efforts help build a culture of accountability and awareness throughout the organization. As water and wastewater utilities contend with growing physical and cybersecurity risks, insider threat management stands as a foundational safeguard for maintaining operational resilience across the all-hazards threat landscape.

CONCLUSION

Ultimately, emerging technologies, rising geopolitical tensions, a growing number of third parties, and other factors have created a threat environment in which water and wastewater utilities can no longer afford to overlook insider risk. Despite all these emerging issues, insider threats remain fundamentally a human problem because they stem from the actions, decisions, and behaviors of employees, contractors, or other trusted insiders, not just technical vulnerabilities. As a result, organizational culture and policies, including leadership and HR, play a critical role in mitigating these risks through careful hiring, ongoing employee engagement, training, performance management, and coordination with security and leadership throughout the employee lifecycle.

Unlike external risks, insider threats originate from individuals with legitimate access—such as employees, contractors, or trusted third parties—who may intentionally or inadvertently compromise sensitive systems or processes. As the water and wastewater sector continues to modernize and adopt increasingly interconnected technologies, insider threats remain a significant and evolving risk to the security and resilience of critical infrastructure.

Consequently, this report has demonstrated that insider threats extend beyond the common conception of malicious insiders to include trusted employees, contractors, and other authorized individuals whose intentional or unintentional actions can compromise the confidentiality, integrity, and availability of essential water and wastewater services. After examining the various types of insider threats, along with recent trends in employee theft, unintentional insider threats, cyber acts, disgruntled employee sabotage, and workplace violence, as well as representative case studies for each category, it is evident that insider incidents can have operational, financial, reputational, and public health consequences.

These findings underscore the need for organizations to adopt a comprehensive insider threat program that integrates physical security, cybersecurity, personnel security, and organizational culture. Implementing proactive mitigation measures—including robust access controls, continuous monitoring, employee awareness training, behavioral reporting mechanisms, and incident response planning—can significantly reduce insider risk and strengthen organizational resilience. As insider threats continue to evolve alongside technological and workforce changes, a risk-informed, multidisciplinary approach will be essential to safeguarding the nation's water and wastewater infrastructure against both current and emerging threats.

RESOURCES

This section includes a list of publicly available online resources that water and wastewater utility owners and operators can leverage to implement and/or strengthen a formal insider threat management program at their organization.

- [CISA - Insider Threat Mitigation Guide](#)
- [CISA - Insider Risk Mitigation Program Evaluation \(IRMPE\)](#)
- [CISA - HR's Role in Preventing Insider Threats Fact Sheet](#)
- [CISA - Resources for Onboarding and Employment Screening Fact Sheet](#)
- [WaterISAC - Physical Security and Resilience Advisory Committee: Insider Threat Management – Fact Sheet](#)
- [NCSC - Insider Threat Mitigation for U.S. Critical Infrastructure Entities](#)

ABOUT THE AUTHORS

Alec Davison

Alec Davison is a Risk Analyst at Gate 15. In that capacity, he also serves as the Lead Risk Analyst at Water Information Sharing and Analysis Center (WaterISAC), where he focuses on physical security, operational resilience, and geopolitical risk. Alec attended George Washington University and received a *master's* degree in Security Policy Studies. He also studied at The Ohio State University, where he received his bachelor's degree in International Studies. He is deeply committed to the Homeland security mission and specifically takes great pride in contributing to the defense of our nation's critical infrastructure.

David Pounder

David Pounder is a Senior Risk Analyst at Gate 15. He has managed insider threat programs at major financial institutions with global footprints. Additionally, he has served as a Business Information Security Office and Vulnerability Assessment Project Manager working to protect mobile applications and sensitive information. Before entering the private sector, he served in the U.S. Army in senior counterintelligence (insider threat) and leadership roles across multiple environments and locations, supporting sensitive operations, investigations, and strategic security programs. With more than 30 years of national security and financial services experience, David specializes in protecting sensitive information, advising senior leaders, and building practical strategies to reduce risk.

REFERENCES

- Alabama Attorney General's Office. (2025, November 20). *Alabama AG indicts Walker County duo for \$680k theft from Providence Water Authority* [Press release]. WBRC. <https://www.wbrc.com/2025/11/20/walker-county-grand-jury-indicts-mother-son-charges-they-stole-hundreds-thousands-dollars-water-authority/>
- AL.com. (2025, April). *Indictment unsealed in Prichard Water Board's multi-million-dollar fraud scheme*. <https://www.al.com/news/2025/04/indictment-unsealed-in-prichard-water-boards-multi-million-dollar-fraud-scheme.html>
- AL.com. (2025, June). *Police investigating copper theft ring involving Birmingham Water Works staff*. <https://www.al.com/news/birmingham/2025/06/police-investigating-copper-theft-ring-involving-birmingham-water-works-staff.html>
- Associated Press. (2016, July 26). *Citibank sabotage gets former employee almost 2 years in prison*. CBS News San Francisco. <https://www.cbsnews.com/sanfrancisco/news/citibank-sabotage-gets-former-employee-almost-2-years-in-prison/>
- City of Virginia Beach, Communications Office. (n.d.). *May 31 investigation*. Retrieved August 4, 2026, from <https://communications.viriniabeach.gov/may-31-investigation>
- Davis, A. (2026, March 5). *Houston Public Works employees accused of using city cards to buy, resell tools*. Click2Houston (KPRC 2). <https://www.click2houston.com/news/local/2026/03/05/houston-public-works-employees-accused-of-using-city-cards-to-buy-resell-tools/>
- Davison, A. (2026, February 5). *(TLP:CLEAR) CISA urges critical infrastructure organizations take action against insider threats, and publishes new product*. WaterISAC. <https://www.waterisac.org/tlpclear-cisa-urges-critical-infrastructure-organizations-take-action-against-insider-threats-and-publishes-new-product>
- Davison, A. (2025, September 30). *(TLP:CLEAR) WaterISAC Physical Security and Resilience Advisory Committee: Insider threat management – Fact sheet*. WaterISAC. <https://www.waterisac.org/tlpclear-waterisac-physical-security-advisory-committee-insider-threat-management-fact-sheet>
- Davison, A. (2026, March 16). *(TLP:CLEAR) WaterISAC – EPA: National Security Information Sharing Bulletin – Q1 2026*. WaterISAC. <https://www.waterisac.org/tlpclear-waterisac-epa-national-security-information-sharing-bulletin-q1-2026>
- Davison, A. (2026, June 10). *(TLP:CLEAR) WaterISAC – EPA: National Security Information Sharing Bulletin – Q2 2026*. WaterISAC.

<https://www.waterisac.org/tlpclear-waterisac-epa-national-security-information-sharing-bulletin-q2-2026>

Defense Counterintelligence and Security Agency, Center for Development of Security Excellence. (n.d.). *National Insider Threat Awareness Month (NITAM)*. Security Awareness Hub. Retrieved August 4, 2026, from <https://securityawareness.dcsa.mil/cdse/nitam/>

Elveborg Lindskog, E., Lioufas, A., & Wagman Kåring, A. (2026). *"Spies among us": Espionage in Europe: A study on convicted spies in Europe 2008-2024* (Report No. FOI-R--5866--SE). Swedish Defence Research Agency (FOI). <https://www.foi.se/rest-api/report/FOI-R--5866--SE>

Federal Bureau of Investigation. (2001, February 18). *Robert Hanssen*. <https://www.fbi.gov/history/famous-cases/robert-hanssen>

Federal Bureau of Investigation, Norfolk Field Office. (2021, June 9). *FBI provides final briefing on the Virginia Beach Municipal Center shooting to the Virginia Beach Police Department* [Press release]. <https://www.fbi.gov/contact-us/field-offices/norfolk/news/press-releases/fbi-provides-final-briefing-on-the-virginia-beach-municipal-center-shooting-to-the-virginia-beach-police-department>

Federal Bureau of Investigation, Environmental Protection Agency, & Internet Crime Complaint Center. (2026, June 3). *Cybersecurity advisory: Threats to U.S. water and wastewater sector facilities* (Alert No. 260603). IC3.gov. <https://www.ic3.gov/CSA/2026/260603.pdf>

FOX 35 Orlando. (n.d.). Florida Port Orange Oak Street Spruce Creek Road hazmat incident evacuations. <https://www.fox35orlando.com/news/florida-port-orange-oak-street-spruce-creek-road-hazmat-incident-evacuations>

ID Agent. (2023, December 23). *3 main motivators behind malicious insider threats have shifted*. <https://www.idagent.com/blog/3-main-motivators-behind-malicious-insider-threats-have-shifted/>

KXII. (2025, January 9). Davis water issue resolved after employee error causes chlorine spike. <https://www.kxii.com/2025/01/09/davis-water-issue-resolved-after-employee-error-causes-chlorine-spike/>

Langrock, S. (2025, November 13). Third-party risk statistics. Recorded Future. <https://www.recordedfuture.com/blog/third-party-risk-statistics>

Maile, A., Rivas, A., Jacobo, J., & Margolin, J. (2019, May 31). 12 killed after gunman opens fire "indiscriminately" at Virginia Beach office: Police. ABC News. <https://abcnews.go.com/US/multiple-people-injured-shooter-custody-virginia-beach-police/story?id=63408118>

- Mimecast. (2026, March 4). *Mimecast study: 42% of organizations report rise in malicious insider threats over past year* [Press release]. <https://www.mimecast.com/resources/press-releases/sohr-26/>
- Ponemon Institute. (2025). *The security risk organizations should not ignore: Careless, negligent and malicious insiders*. <https://www.ponemon.org/news-updates/blog/security/the-security-risk-organizations-should-not-ignore-careless-negligent-and-malicious-insiders.html>
- Pollock, T. (2025, November 20). Walker County mother, son indicted on charges they stole from water authority. WBRC. <https://www.wbrc.com/2025/11/20/walker-county-grand-jury-indicts-mother-son-charges-they-stole-hundreds-thousands-dollars-water-authority/>
- Proofpoint, Inc. (2026). *2026 AI and human risk landscape report*. <https://www.proofpoint.com/us/resources/threat-reports/ai-human-risk-landscape-report>
- SentinelOne. (2026, May 6). *Insider threat statistics for 2026*. <https://www.sentinelone.com/cybersecurity-101/cybersecurity/insider-threat-statistics/>
- Snow, C. (2025, July 10). (TLP:CLEAR) Cross-sector ISAC report: Threat overview and mitigations for the North Korea IT worker problem. WaterISAC. <https://www.waterisac.org/tlpclear-cross-sector-isac-report-threat-overview-and-mitigations-north-korea-it-worker>
- Software Engineering Institute. (2022, September 7). *Common sense guide to mitigating insider threats* (7th ed.). Carnegie Mellon University. <https://www.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/>
- The Enterprise. (2024, March 8). Stoughton town employee, Brockton man Robert Bullock, charged federally with tampering with water supply. <https://www.enterpriseneews.com/story/news/crime/2024/03/08/stoughton-town-employee-brockton-man-robert-bullock-charged-federally-tampering-water-supply/72893909007/>
- Treon, C. (2026, September 1). Texas Cyber Command joins federal water sector cybersecurity pilot. Industry Insider Texas. <https://insider.govtech.com/texas/news/texas-cyber-command-joins-federal-water-sector-cybersecurity-pilot>
- U.S. Attorney's Office, District of Kansas. (2021, October 20). *Kansas man pleads guilty to water facility tampering* [Press release]. <https://www.justice.gov/usao-ks/pr/kansas-man-pleads-guilty-water-facility-tampering>

- U.S. Attorney's Office, Southern District of Alabama. (2025, April 3). *Indictment unsealed charging multi-million dollar fraud scheme at Prichard Water Board* [Press release]. U.S. Department of Justice. <https://www.justice.gov/usao-sdal/pr/indictment-unsealed-charging-multi-million-dollar-fraud-scheme-prichard-water-board>
- U.S. Attorney's Office, District of Massachusetts. (2025, March 26). *Former Stoughton Water Department employee pleads guilty to tampering with drinking water* [Press release]. U.S. Department of Justice. <https://www.justice.gov/usao-ma/pr/former-stoughton-water-department-employee-pleads-guilty-tampering-drinking-water>
- U.S. Cybersecurity and Infrastructure Security Agency. (2020, November). *Insider threat mitigation guide*. https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
- U.S. Department of Justice, Office of the U.S. Attorney, Northern District of California. (2023, July 6). *Tracy resident charged with computer attack on Discovery Bay water treatment facility* [Press release]. <https://www.justice.gov/usao-ndca/pr/tracy-resident-charged-computer-attack-discovery-bay-water-treatment-facility>
- U.S. Department of Justice, Office of Public Affairs. (2025, February 6). *Florida telecommunications and information technology worker pleads guilty to conspiring to act as agent of PRC government* [Press release]. <https://www.justice.gov/opa/pr/florida-telecommunications-and-information-technology-worker-pleads-guilty-conspiring-act>
- U.S. Department of Justice, Office of Public Affairs. (2025, April 16). *Former FAA contractor pleads guilty to illegally acting as an agent of the Iranian government* [Press release]. <https://www.justice.gov/opa/pr/former-faa-contractor-pleads-guilty-illegally-acting-agent-iranian-government>
- Voice of America. (n.d.). *VOA special report: History of mass shooters – Workplace shootings*. Retrieved August 4, 2026, from <https://projects.voanews.com/mass-shootings/english/locations/workplace.html>
- Waldman, A. (2026, September 1). Stronger security drives ransomware groups to recruit from within. Dark Reading. <https://www.darkreading.com/cyber-risk/stronger-security-drives-ransomware-groups-to-recruit-from-within>
- WaterISAC. (2024, December 19). Cybersecurity fundamentals for water and wastewater utilities, WaterISAC, <https://www.waterisac.org/fundamentals>
- WBRC. (2026, February 12). *(TLP:CLEAR) Ransomware attack at payment platform provider BridgePay causes disruptions at water utilities nationwide* (C. Snow, Author). WaterISAC. <https://www.waterisac.org/tlpclear-ransomware-attack-at->

payment-platform-provider-bridgepay-causes-disruptions-at-water-utilities-nationwide

- WHTM (ABC27). (2025, February 26). *Former Lancaster County township employee allegedly made bomb threat, threatened staff*. <https://www.abc27.com/local-news/former-lancaster-county-township-employee-allegedly-made-bomb-threat-threatened-staff/>
- WKTV. (2024, October 7). *Police: \$14,000 in copper wire stolen from local water plant; Clinton man arrested for grand larceny*. https://www.wktv.com/news/crime/police-14-000-in-copper-wire-stolen-from-local-water-plant-clinton-man-arrested-for/article_b8677e6a-84d6-11ef-8ca0-1391dc87ad33.html

ENDNOTES

- ⁱ A. Davison, "(TLP:CLEAR) CISA Urges Critical Infrastructure Organizations Take Action Against Insider Threats, and Publishes New Product," WaterISAC, February 5, 2026, <https://www.waterisac.org/tlpclear-cisa-urges-critical-infrastructure-organizations-take-action-against-insider-threats-and-publishes-new-product>.
- ⁱⁱ U.S. Cybersecurity and Infrastructure Security Agency, *Insider Threat Mitigation Guide* (Washington, DC: CISA, November 2020), https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.
- ⁱⁱⁱ SentinelOne, "Insider Threat Statistics for 2026," May 6, 2026, <https://www.sentinelone.com/cybersecurity-101/cybersecurity/insider-threat-statistics/>.
- ^{iv} Proofpoint, Inc., *2026 AI and Human Risk Landscape Report* (2026), <https://www.proofpoint.com/us/resources/threat-reports/ai-human-risk-landscape-report>.
- ^v WaterISAC, "Cybersecurity Fundamentals for Water and Wastewater Utilities," December 19, 2024, <https://www.waterisac.org/fundamentals>.
- ^{vi} CISA, *Insider Threat Mitigation Guide*.
- ^{vii} *Ibid.*

-
- viii E. Elveborg Lindskog, A. Lioufas, and A. Wagman Kåring, "Spies among Us": Espionage in Europe: A Study on Convicted Spies in Europe 2008–2024, report no. FOI-R--5866--SE (Swedish Defence Research Agency [FOI], 2026), <https://www.foi.se/rest-api/report/FOI-R--5866--SE>.
- ix Federal Bureau of Investigation, "Robert Hanssen," February 18, 2001, <https://www.fbi.gov/history/famous-cases/robert-hanssen>.
- x CISA, Insider Threat Mitigation Guide.
- xi Associated Press, "Citibank Sabotage Gets Former Employee Almost 2 Years in Prison," *CBS News San Francisco*, July 26, 2016, <https://www.cbsnews.com/sanfrancisco/news/citibank-sabotage-gets-former-employee-almost-2-years-in-prison/>.
- xii Voice of America, "VOA Special Report: History of Mass Shooters—Workplace Shootings," accessed August 4, 2026, <https://projects.voanews.com/mass-shootings/english/locations/workplace.html>.
- xiii A. Davison, "(TLP:CLEAR) WaterISAC–EPA: National Security Information Sharing Bulletin–Q1 2026," *WaterISAC*, March 16, 2026, <https://www.waterisac.org/tlpclear-waterisac-epa-national-security-information-sharing-bulletin-q1-2026>.
- xiv A. Waldman, "Stronger Security Drives Ransomware Groups to Recruit from Within," *Dark Reading*, September 1, 2026, <https://www.darkreading.com/cyber-risk/stronger-security-drives-ransomware-groups-to-recruit-from-within>.
- xv S. Langrock, "Third-Party Risk Statistics," *Recorded Future*, November 13, 2025, <https://www.recordedfuture.com/blog/third-party-risk-statistics>.
- xvi Ponemon Institute, "The Security Risk Organizations Should Not Ignore: Careless, Negligent and Malicious Insiders," 2025, <https://www.ponemon.org/news-updates/blog/security/the-security-risk-organizations-should-not-ignore-careless-negligent-and-malicious-insiders.html>.
- xvii Mimecast, "Mimecast Study: 42% of Organizations Report Rise in Malicious Insider Threats over Past Year," press release, March 4, 2026, <https://www.mimecast.com/resources/press-releases/sohr-26/>.
- xviii Ponemon Institute, "The Security Risk Organizations Should Not Ignore."
- xix A. Davison, "(TLP:CLEAR) WaterISAC – EPA: National Security Information Sharing Bulletin – Q2 2026," *WaterISAC*, June 10, 2026, <https://www.waterisac.org/tlpclear-waterisac-epa-national-security-information-sharing-bulletin-q2-2026>.

-
- ^{xx} WBRC, "(TLP:CLEAR) Ransomware Attack at Payment Platform Provider BridgePay Causes Disruptions at Water Utilities Nationwide," by C. Snow, *WaterISAC*, February 12, 2026, <https://www.waterisac.org/tlpclear-ransomware-attack-at-payment-platform-provider-bridgepay-causes-disruptions-at-water-utilities-nationwide>.
- ^{xxi} Davison, "WaterISAC – EPA: National Security Information Sharing Bulletin – Q2 2026."
- ^{xxii} ID Agent, "3 Main Motivators Behind Malicious Insider Threats Have Shifted," December 23, 2023, <https://www.idagent.com/blog/3-main-motivators-behind-malicious-insider-threats-have-shifted/>.
- ^{xxiii} *Ibid.*
- ^{xxiv} Federal Bureau of Investigation, Environmental Protection Agency, and Internet Crime Complaint Center, "Cybersecurity Advisory: Threats to U.S. Water and Wastewater Sector Facilities," Alert No. 260603, IC3.gov, June 3, 2026, <https://www.ic3.gov/CSA/2026/260603.pdf>.
- ^{xxv} U.S. Department of Justice, Office of Public Affairs, "Florida Telecommunications and Information Technology Worker Pleads Guilty to Conspiring to Act as Agent of PRC Government," press release, February 6, 2025, <https://www.justice.gov/opa/pr/florida-telecommunications-and-information-technology-worker-pleads-guilty-conspiring-act>.
- ^{xxvi} U.S. Department of Justice, Office of Public Affairs, "Former FAA Contractor Pleads Guilty to Illegally Acting as an Agent of the Iranian Government," press release, April 16, 2025, <https://www.justice.gov/opa/pr/former-faa-contractor-pleads-guilty-illegally-acting-agent-iranian-government>.
- ^{xxvii} C. Snow, "(TLP:CLEAR) Cross-Sector ISAC Report: Threat Overview and Mitigations for the North Korea IT Worker Problem," *WaterISAC*, July 10, 2025, <https://www.waterisac.org/tlpclear-cross-sector-isac-report-threat-overview-and-mitigations-north-korea-it-worker>.
- ^{xxviii} *Ibid.*
- ^{xxix} KXII, "Davis Water Issue Resolved after Employee Error Causes Chlorine Spike," January 9, 2025, <https://www.kxii.com/2025/01/09/davis-water-issue-resolved-after-employee-error-causes-chlorine-spike/>.
- ^{xxx} FOX 35 Orlando, "Florida Port Orange Oak Street Spruce Creek Road Hazmat Incident Evacuations," accessed September 10, 2026, <https://www.fox35orlando.com/news/florida-port-orange-oak-street-spruce-creek-road-hazmat-incident-evacuations>.

-
- xxxvi WKTV, "Police: \$14,000 in Copper Wire Stolen from Local Water Plant; Clinton Man Arrested for Grand Larceny," October 7, 2024, https://www.wktv.com/news/crime/police-14-000-in-copper-wire-stolen-from-local-water-plant-clinton-man-arrested-for/article_b8677e6a-84d6-11ef-8ca0-1391dc87ad33.html.
- xxxvii AL.com, "Indictment Unsealed in Prichard Water Board's Multi-Million-Dollar Fraud Scheme," April 2025, <https://www.al.com/news/2025/04/indictment-unsealed-in-prichard-water-boards-multi-million-dollar-fraud-scheme.html>.
- xxxviii T. Pollock, "Walker County Mother, Son Indicted on Charges They Stole from Water Authority," WBRC, November 20, 2025, <https://www.wbrc.com/2025/11/20/walker-county-grand-jury-indicts-mother-son-charges-they-stole-hundreds-thousands-dollars-water-authority/>.
- xxxix U.S. Attorney's Office, District of Kansas, "Kansas Man Pleads Guilty to Water Facility Tampering," press release, October 20, 2021, <https://www.justice.gov/usao-ks/pr/kansas-man-pleads-guilty-water-facility-tampering>.
- xl U.S. Department of Justice, Office of the U.S. Attorney, Northern District of California, "Tracy Resident Charged with Computer Attack on Discovery Bay Water Treatment Facility," press release, July 6, 2023, <https://www.justice.gov/usao-ndca/pr/tracy-resident-charged-computer-attack-discovery-bay-water-treatment-facility>.
- xli WHTM (ABC27), "Former Lancaster County Township Employee Allegedly Made Bomb Threat, Threatened Staff," February 26, 2025, <https://www.abc27.com/local-news/former-lancaster-county-township-employee-allegedly-made-bomb-threat-threatened-staff/>.
- xlii U.S. Attorney's Office, District of Massachusetts, "Former Stoughton Water Department Employee Pleads Guilty to Tampering with Drinking Water," press release, U.S. Department of Justice, March 26, 2025, <https://www.justice.gov/usao-ma/pr/former-stoughton-water-department-employee-pleads-guilty-tampering-drinking-water>.
- xliiii The Enterprise, "Stoughton Town Employee, Brockton Man Robert Bullock, Charged Federally with Tampering with Water Supply," March 8, 2024, <https://www.enterpriseneeds.com/story/news/crime/2024/03/08/stoughton-town-employee-brockton-man-robert-bullock-charged-federally-tampering-water-supply/72893909007/>.
- xliv Amanda Maile et al., "12 Killed after Gunman Opens Fire 'Indiscriminately' at Virginia Beach Office: Police," ABC News, May 31, 2019,

<https://abcnews.go.com/US/multiple-people-injured-shooter-custody-virginia-beach-police/story?id=63408118>.

- ^{xi} Federal Bureau of Investigation, Norfolk Field Office. (2021, June 9). FBI provides final briefing on the Virginia Beach Municipal Center shooting to the Virginia Beach Police Department [Press release]. <https://www.fbi.gov/contact-us/field-offices/norfolk/news/press-releases/fbi-provides-final-briefing-on-the-virginia-beach-municipal-center-shooting-to-the-virginia-beach-police-department>
- ^{xli} SentinelOne, "Insider Threat Statistics for 2026."
- ^{xlii} Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*, 7th ed. (Pittsburgh: Carnegie Mellon University, September 7, 2022), <https://www.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/>.
- ^{xliii} CISA, Insider Threat Mitigation Guide.
- ^{xliv} WaterISAC, "Cybersecurity Fundamentals for Water and Wastewater Utilities."
- ^{xliv} City of Virginia Beach, Communications Office, "May 31 Investigation," accessed August 4, 2026, <https://communications.virginiabeach.gov/may-31-investigation>.
- ^{xlvi} C. Treon, "Texas Cyber Command Joins Federal Water Sector Cybersecurity Pilot," Industry Insider Texas, September 1, 2026, <https://insider.govtech.com/texas/news/texas-cyber-command-joins-federal-water-sector-cybersecurity-pilot>.
- ^{xlvi} A. Davison, "(TLP:CLEAR) WaterISAC Physical Security and Resilience Advisory Committee: Insider Threat Management – Fact Sheet," WaterISAC, September 30, 2025, <https://www.waterisac.org/tlpclear-waterisac-physical-security-advisory-committee-insider-threat-management-fact-sheet>.
- ^{xlvi} Defense Counterintelligence and Security Agency, Center for Development of Security Excellence, "National Insider Threat Awareness Month (NITAM)," Security Awareness Hub, accessed August 4, 2026, <https://securityawareness.dcsa.mil/cdse/nitam/>.

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.

Davison, A., Pounder, D., (2026). Insider Threats in the Water Sector A Growing and Underestimated Risk. (Report No. 2026 - 1040). Sam

Houston State University Institute for Homeland Security.

<https://doi.org/10.17605/OSF.IO/JK3WH>



**INSTITUTE FOR
HOMELAND SECURITY**
SAM HOUSTON STATE UNIVERSITY

