resilience

REPORT

Cyber risk in energy and utilities

What insurance claims data reveals about controls that were already in place

Cyber risk in energy and utilities

What insurance claims data reveals about controls that were already in place

Executive summary

Several of the failures in these claims involved controls the client already deployed.

This paper examines cyber claims analysis from Resilience's portfolio in energy and utilities and the unique aspects of threats and losses in this sector. Energy accounts diverge from the rest of our portfolio most notably on cause of loss. Across the claims in our oil and energy, utilities, and renewables accounts filed from January 1, 2023 through September 5, 2026, email compromise accounts for 21% of claims, compared to 10% everywhere else. Across all claims on record, it accounts for 2% of energy's incurred losses including reserves, compared to 4% in the rest of the portfolio. Ransomware makes up roughly 70% of energy's incurred losses, about the same share as in the rest of the portfolio.

In the specific cases we took a look at, attackers beat controls clients had already switched on. One talked an employee into entering a password and a one-time code on a fake login page. Another took over a live session that was already authenticated. Clients with recently tested backups recovered without paying, and clients who had separated their operational systems from corporate IT kept production running.

None of our clients has filed a claim tied to the 2026 campaign against water and wastewater utilities. An attacker can sit in a control system for months without disrupting anything, which leaves nobody a reason to file. Claims data undercounts that activity, so testing your own controls is where the answer has to come from.

Test them against the failures these claims show. Run the multifactor authentication (MFA) workarounds that turn up in our claims, and restore from a backup an attacker holding your credentials couldn't have reached. For operational systems, check whether any controller is reachable from the internet and find out how long you could keep running manually. Then ask each vendor what its outage or breach would cost you. For one that runs or maintains your equipment, start with lost revenue.

Key findings

Energy's biggest gap is email compromise

Email compromise, malware, and ransomware each make up a larger share of energy's claims than of claims across the rest of the portfolio. The largest of those gaps is in email compromise, at 11 points, yet email compromise accounts for only 2% of energy's incurred losses including reserves.

Attackers got around controls that were already running

In several of the email compromise claims we read, attackers worked around MFA that was already switched on, largely through social engineering. In the ransomware claims, recently tested immutable backups let clients recover without paying, and in two cases segmentation kept production running.

Vendor incidents account for a smaller share of energy's claims

In 17% of energy's claims, the incident started at a vendor, compared to 24% across the rest of the portfolio. About a third of those vendors were HR, payroll, benefits, or accounting firms, and the rest included engineering, brokerage, energy-services, billing, payments, IT, and web-hosting vendors. In one claim, a client lost income when ransomware hit the vendor that operated its equipment, and a single incident at a shared service produced claims from two utility clients.

None of our energy claims involve control system manipulation

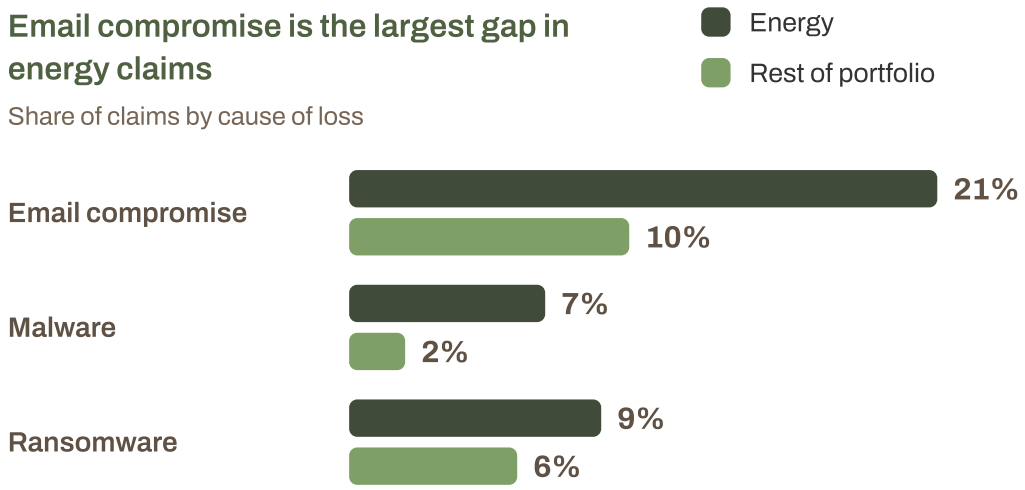
We have water and wastewater utility clients, and none of them filed a claim while attackers in the 2026 campaign were hitting utilities in at least seven states. That absence is about what claims capture. Anyone sizing operational technology risk from claims data is working from an undercount, which is why clients have to test those controls directly.

Email compromise, malware, and ransomware make up more of energy's claims

Energy sector cyber risk, as we measure it, covers our oil and energy, utilities, and renewables accounts together. Email compromise is the largest single separation in the loss mix, at 21% of energy account claims compared to 10% everywhere else. Malware is a small share in both segments, and energy's is five points higher, 7% compared to 2%. The gap is smallest for ransomware, 9% compared to 6%. Weighted by dollars across all claims on record, email compromise is 2% of energy's incurred losses including reserves, compared to 4% for the rest of the portfolio.

Email compromise is the largest gap in energy claims

Share of claims by cause of loss



Resilience claims, Jan. 1, 2023 – Sept. 5, 2026. Shares are within each segment.

> Email compromise is the largest single separation in the loss mix, at 21% of energy account claims compared to 10% everywhere else.

Attackers got around controls that were already running

In several of these claims, MFA was switched on, so attackers went after the person using it or the session behind it instead. One attacker talked an employee into entering a password and a one-time code on a fake page they controlled, and captured both at once. Another hijacked a session that had already passed the MFA check and used it to register a new MFA method of their own, so they could sign back in later.

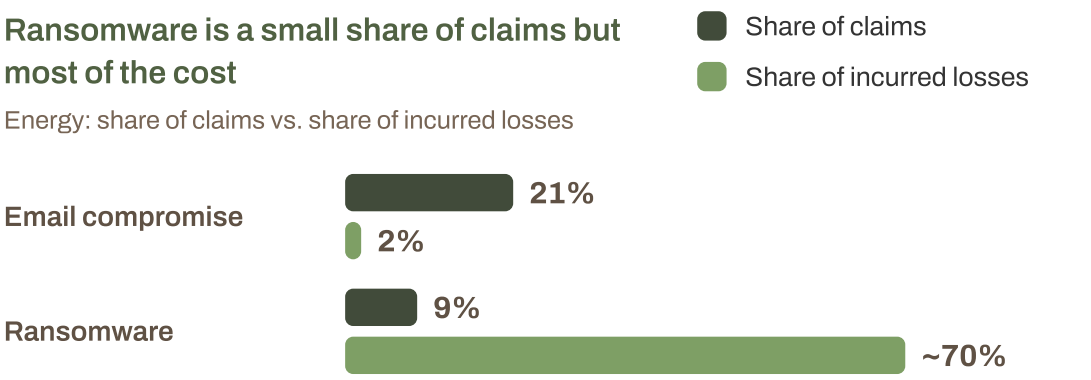
Ransomware makes up about 70% of energy's incurred losses, and the ransomware claims show a mixed record on controls.

At two companies, clients had recent backups they had tested and found clean, so they had little reason to pay, and they recovered from those copies.

In one claim, ransomware reached supervisory control and data acquisition (SCADA) systems knocked out communications, and left the client without visibility over equipment that was still physically running. In the other two cases, the operational systems ran on a separate, segmented network the attacker never reached, so production carried on through an IT compromise.

Ransomware is a small share of claims but most of the cost

Energy: share of claims vs. share of incurred losses



Resilience claims. Losses incurred including reserves, from claims with a recorded amount.

> In several of these claims, MFA was switched on, so attackers went after the person using it or the session behind it instead.

Energy's claims start with a vendor less often than the rest of the portfolio's

The two vendor categories, vendor data breach and ransomware impacting a vendor, together account for 17% of energy claims, compared to 24% across the rest of the portfolio.

About a third of energy's vendor claims involved HR platforms, payroll processors, benefits administrators, or accounting firms, the vendors any employer uses. Several of those resulted from the 2023 MOVEit Transfer vulnerability that Progress Software disclosed[1] and the 2024 Change Healthcare breach documented by the HHS Office for Civil Rights[2], two events that affected companies in every sector. An energy company shows up in those claims because it employs people and pays them through a vendor. The rest involved engineering, brokerage, energy-services, billing, payments, IT, and web-hosting vendors.

Ransomware makes up about 70% of energy's incurred losses, and the ransomware claims divide cleanly. At two companies, clients had recent backups they had tested and found clean, so they had little reason to pay, and they recovered from those copies. At two more, operational systems

ran on a separate, segmented network the attacker never reached, so production carried on through an IT compromise. In one claim, ransomware reached supervisory control and data acquisition (SCADA) systems, knocked out communications, and left the client without visibility over equipment that was still physically running.

Fewer energy claims start at a vendor

Share of claims that began as a vendor breach or vendor ransomware



Resilience claims, Jan. 1, 2023 – Sept. 5, 2026.

An attacker can sit in a control system for months without disrupting anything.

The 2026 water utility attacks ran on shared controllers

When many organizations run the same product, one flaw reaches all of them at once. In 2023, a flaw in one widely deployed file transfer product let unauthenticated attackers reach its database at any organization running an affected version.[1] Our own vendor claims from that one event span unrelated clients in unrelated sectors. Controllers work the same way, with one exposed model standing in for the shared product.

Our Risk Operations Center (ROC) has been tracking a campaign against water and wastewater utilities in which attackers have compromised utilities across the sector through the same exposed equipment and similar third-party network setups.

By July 30, 2026, water and wastewater utilities in at least seven states had reported incidents to the FBI3. In some of those incidents, attackers disrupted water operations. Attackers reached controllers exposed directly to the public internet and changed their IP addresses and passwords, which left operators without a view of connected equipment and, in some cases, without control of it. At least one organization found modified controller project files after noticing discrepancies in ladder logic across several of its sites. How much an attacker could do depended on what the controller ran and whether the utility could fall back on manual operation.

Minnesota IT Services reported a coordinated attack on operational technology at more than 30 community water systems on July 26 and 27, 2026, and has not attributed it to any actor.4 We don't know whether the Minnesota attack is part of the activity in the FBI's reporting. The FBI noted that third parties had set up several victims' networks in similar ways, which may let an attacker who succeeds at one customer repeat it at others.[3]

CISA warned of the same pattern in late November 2023, when attackers were exploiting one manufacturer's controller line in water and wastewater systems and reaching devices on the open internet that still used the manufacturer's default password.[5]

In April 2026, six federal agencies (the FBI, CISA, NSA, EPA, the Department of Energy, and US Cyber Command's Cyber National Mission Force) warned, in a joint advisory, that Iranian-affiliated actors were exploiting internet-exposed controllers at water and wastewater systems, energy facilities, and government sites[6]. On July 22, 2026, they widened it from one manufacturer's controllers to three. Our utilities code includes water and wastewater utilities, and none of their claims involve control system manipulation.

Top ransomware groups draw few victims from energy

Share of each group's victims in energy and utilities



Source: Cyfirma, Energy & Utilities Q1 2026 Industry Report (Feb. 3, 2026). External data, not Resilience claims.

Why control system attacks rarely generate insurance claims

A control system attack rarely produces a claim, because claims data only records events that someone reported under a cyber policy.

An attacker who gets onto a controller and waits makes no ransom demand and encrypts nothing. And if the attacker doesn't take regulated personal data, the utility has no notification obligation either. An intruder running an espionage operation can sit inside a utility for months, however serious the breach, and leave nothing for anyone to file.

On the IT side, claims show clearly where the money goes, and ransomware makes up about 70% of energy's incurred losses. In threat intelligence firm Cyfirma's first-quarter 2026 energy and utilities report, the two ransomware groups with the most victims in the sector, Qilin and Akira, drew only 3.4% and 4.8% of their victims from energy and utilities, a pattern Cyfirma reads as opportunistic targeting.[7] But anyone sizing OT risk from claims data, ours or any other portfolio's, is working from an undercount. Our Risk Operations Center reached the same conclusion independently of the claims review in this report.

Test whether a control holds under attack

To test a control, try to beat it the way an attacker would, and record what happens.

For MFA, that means knowing which factor types your implementation accepts and what your systems do with a session that is already authenticated. You can test each failure point in these claims. An attacker can talk someone on your staff into entering a one-time code on a page that looks like yours. An attacker with a stolen session token can get past a login that never re-prompts. Someone using an account that's already signed in can often register a new MFA method, and so can a help desk agent following a reset script. Attackers relay push approvals and one-time codes, but they have a harder time relaying phishing-resistant factors, so find out which of your applications still fall back to the weaker ones. Check, too, whether older mail protocols such as IMAP and POP still accept a password without MFA, and whether users can grant a third-party app access to their mailbox without review.

Test backups and segmentation the same way you test MFA. Restore from a copy that an attacker holding domain credentials could not have reached or deleted, under something close to live incident conditions. That's why the copy needs to be offsite and immutable, since a backup an attacker can reach can be encrypted along with everything else. Then assume corporate IT is fully compromised and watch whether the operational systems keep running, including the paths people reach for under pressure — the engineering workstation, the vendor's remote access route, and the shared credential that exists so somebody can fix things at two in the morning.

Ask vendors different questions depending on what they do for you. A vendor that holds your data should be able to tell you what data it has, where that data goes, and how it would notify you of a compromise.

With a vendor that operates or maintains your equipment, find out how much revenue you lose while the vendor is down and how long your own staff can keep the equipment running without it. Then check that the vendor's access into your environment is limited to the job it does. Many vendors will need to answer both sets of questions.

On shared sector infrastructure, ask which third parties your peers also depend on, and whether one event at any of them has already produced disruption at more than one of you at the same time. And practice running operational systems manually, which the FBI and EPA recommend.[3]

Claims can't show you whether an attacker is already inside your control networks, so look there directly. Inventory what is reachable from the public internet, then compare controller logic against a known-good baseline, which is how the organization in the FBI and EPA reporting caught its modified project files.[3] Configuration and credential changes on devices nobody should be touching remotely are the other thing to watch.



Use the multifactor authentication (MFA) workarounds that show up in our claims



Try to restore files from a backup an attacker couldn't have reached



Check that no controller is reachable from the internet and see how long you can keep operations running manually



Ask each vendor what it would cost you if it went down or got breached

What this changes

Several of the failures in these claims involved controls the client already deployed, and a controls inventory would have listed them as in place. Ask your team when it last watched one of your controls fail under test, and whether anybody was in the room.

Methodology

Cause-of-loss proportions in this report come from Resilience's claims records for accounts in three industry codes read as one population: oil and energy, utilities, and renewables and environment. The utilities code covers water and wastewater systems. Energy proportions are compared to claims from every other segment in the portfolio over the same period.

The period covered for cause-of-loss proportions is Jan. 1, 2023 through Sept. 5, 2026. Claims with earlier loss dates are excluded because the energy segment has too few from 2021 and 2022 to describe those years.

Cause-of-loss shares are calculated within each segment, as a share of that segment's own claims. The energy figures and the rest-of-portfolio figures are separately normalized and are not shares of a common total.

Loss figures are reported as incurred losses including reserves, the house measure, which estimates a claim's final cost and includes amounts not yet paid. Severity shares are shares of that total by cause of loss, calculated within each segment across all claims on record, including those with loss dates before 2023. They are calculated from the subset of claims carrying a recorded incurred amount, a small fraction of each segment's claims, so they are less reliable than the cause-of-loss shares.

The findings on controls and on the kinds of vendors involved come from reading claim narratives, because the structured fields that would record how an incident started are largely unpopulated.

The review covered every energy email compromise claim in the period and every energy ransomware and vendor-related claim on record. These findings describe what those claims show and are not measured rates.

Average severity is excluded, because at this claim count a single outlier changes it substantially. Individual ransom and settlement amounts are excluded. One vendor severity figure is excluded because its recorded incurred and paid amounts remain unreconciled, which reads as an open reserve.

Extraction and refining are not separable within the oil and energy code. No distinct refining classification exists in this data, and fewer than 1% of companies in that code carry any refining-related code, so the oil and energy figures here describe the general population.

External threat intelligence comes from the public advisories in the endnotes and from our Risk Operations Center. Internal claims analysis and external intelligence are reported separately and are not combined into any figure.

Endnotes

1. Progress Software, “MOVEit Transfer Critical Vulnerability (May 2023), CVE-2023-34362,” May 31, 2023. https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

2. U.S. Department of Health and Human Services, Office for Civil Rights, "Change Healthcare Cybersecurity Incident Frequently Asked Questions," updated March 14, 2025. https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html

3. Federal Bureau of Investigation and Environmental Protection Agency, Public Service Announcement I-073026-PSA, “Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing Programmable Logic Controllers, Causing Operational Disruptions,” July 30, 2026. https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet--facing-programmable-logic-controllers-causing-operational-disruptions

4. Minnesota IT Services, “Minnesota continues response to cyber activity affecting community water systems,” July 30, 2026. https://mn.gov/mnit/media/blog/?id=38-762209

5. Cybersecurity and Infrastructure Security Agency, “Exploitation of Unitronics PLCs used in Water and Wastewater Systems,” Nov. 28, 2023. https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

6. Joint Cybersecurity Advisory AA26-097A, "Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure," FBI, CISA, NSA, EPA, DOE, and US Cyber Command Cyber National Mission Force, April 7, 2026, updated July 22, 2026. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

7. Cyfirma, "Energy & Utilities Q1 2026: Industry Report," Feb. 3, 2026. https://www.cyfirma.com/research/energy-utilities-q1-2026-industry-report/

This material is provided for informational purposes only. Accordingly, this material should not be viewed as a substitute for guidance and recommendations of a trained professional. Additionally, Arceo Labs, Inc. d/b/a Resilience does not endorse any coverage, systems, processes, or protocols addressed herein. Any references to non-Resilience websites are provided solely for convenience, and Resilience disclaims any responsibility with respect to such websites. To the extent that this material contains any examples, please note that they are for illustrative purposes only. Additionally, examples are not intended to establish any standard of care, to serve as legal advice appropriate for any factual situation, or to provide an acknowledgment that any factual situation is covered by Resilience products. This material is not intended as a solicitation of insurance coverage. Arceo Labs, Inc. d/b/a Resilience, 55 2nd St Suite 1950, San Francisco, CA 94105. All Rights Reserved.