semperis

The State of Critical Infrastructure Resilience

Evaluating Cyber Threats to Water and Electric Utilities

- Cyber threats pose a growing risk to utility operators — and public safety.
- Nation-state actors are behind most breaches and are adept at remaining undetected.
- Identity systems remain a top target for initial access and escalation.
- Both publicly and privately operated utilities can better adapt to these threats by adopting a resilience mindset.

"The technology and systems that deliver critical services like power grids and drinking water underpin every facet of our health and safety. Far too many people assume that the government or private sector companies are managing the essential task of addressing the resilience of these systems. This is a flawed assumption, borne out by frequent systemic failures of poorly designed and weakly defended systems that are easy prey for criminals and rogue nation states. This responsibility cannot be deferred to others. We need to harden our systems and extract criminal elements — now."

Chris Inglis

Former US National Cyber Director
Strategic Advisor, Semperis

Executive **Summary**

Reliable access to fresh water and adequate electricity is a critical component of daily life in the United States and United Kingdom. As recent outages — driven by environmental catastrophes, human error, or cyberattacks — have shown, even short disruptions to these services have the potential for social and economic harm.

Ransomware groups and nation-states such as China, Russia, Iran, and North Korea — all known to be advanced persistent threat actors — are well aware of this fact. The question is not whether critical utility infrastructure in the US and UK poses a cyberattack target. The question is: **How prepared are utility operators to detect, respond to, and recover from cyberattacks?**

To gauge the answer, Semperis conducted a survey of information technology (IT) and security professionals at 350 water treatment plants and electricity operators in the US and UK. This report reveals crucial lessons for any publicly or privately operated utility supporting critical national infrastructure.

> "Part of the Chinese cyber threat that has not gotten the public attention it deserves is that the Chinese government is pre-positioning on American civilian critical infrastructure. They're lying in wait on those networks to inflict real-world harm at a time and place of their choosing."
>
> **Christopher Wray**
> Former FBI Director

Executive **Summary**

Key Findings

62% said their organizations had been targeted by threat actors in the past 12 months, and **80% of those were attacked multiple times**.

59% confirmed that **nation-state-sponsored cyber criminals were behind the attacks**, yet experts agree that many more might simply lack the ability to detect stealthier attacks.

57% of attacks disrupted normal operations, with **54%** of victims suffering **permanent corruption or destruction** of data or systems.

82% of attacks **definitely or possibly compromised Tier 0 identity systems**, such as Active Directory, Entra ID, and Okta.

CONTRIBUTING EXPERTS

Simon Hodgkinson
Former bp Chief Information Security Officer (CISO)
Semperis Strategic Advisor

Chris Inglis
Former US National Cyber Director
Semperis Strategic Advisor

Ciaran Martin, CB
Paladin Capital Group Managing Director, founding Chief Executive of the UK's National Cyber Security Centre

Mickey Bresman
Semperis CEO

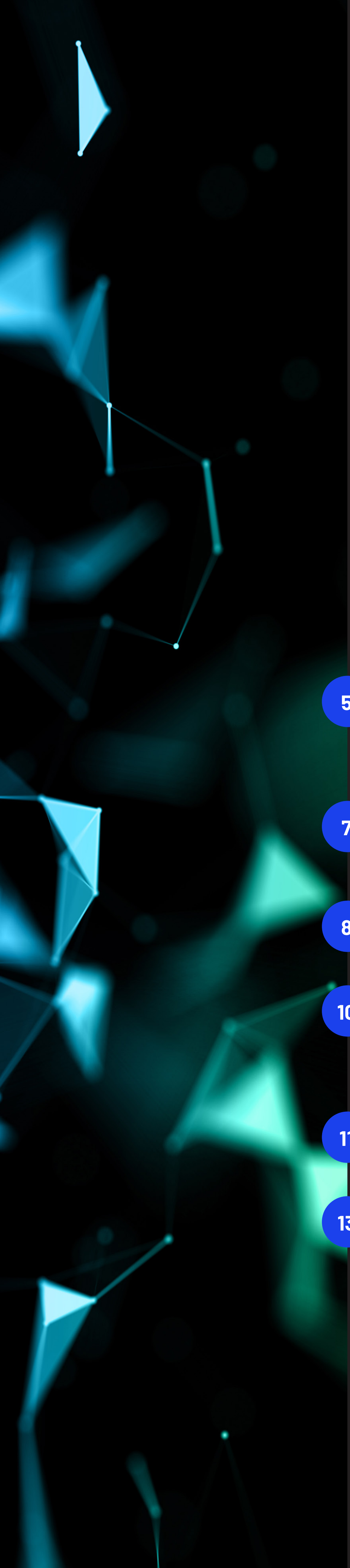
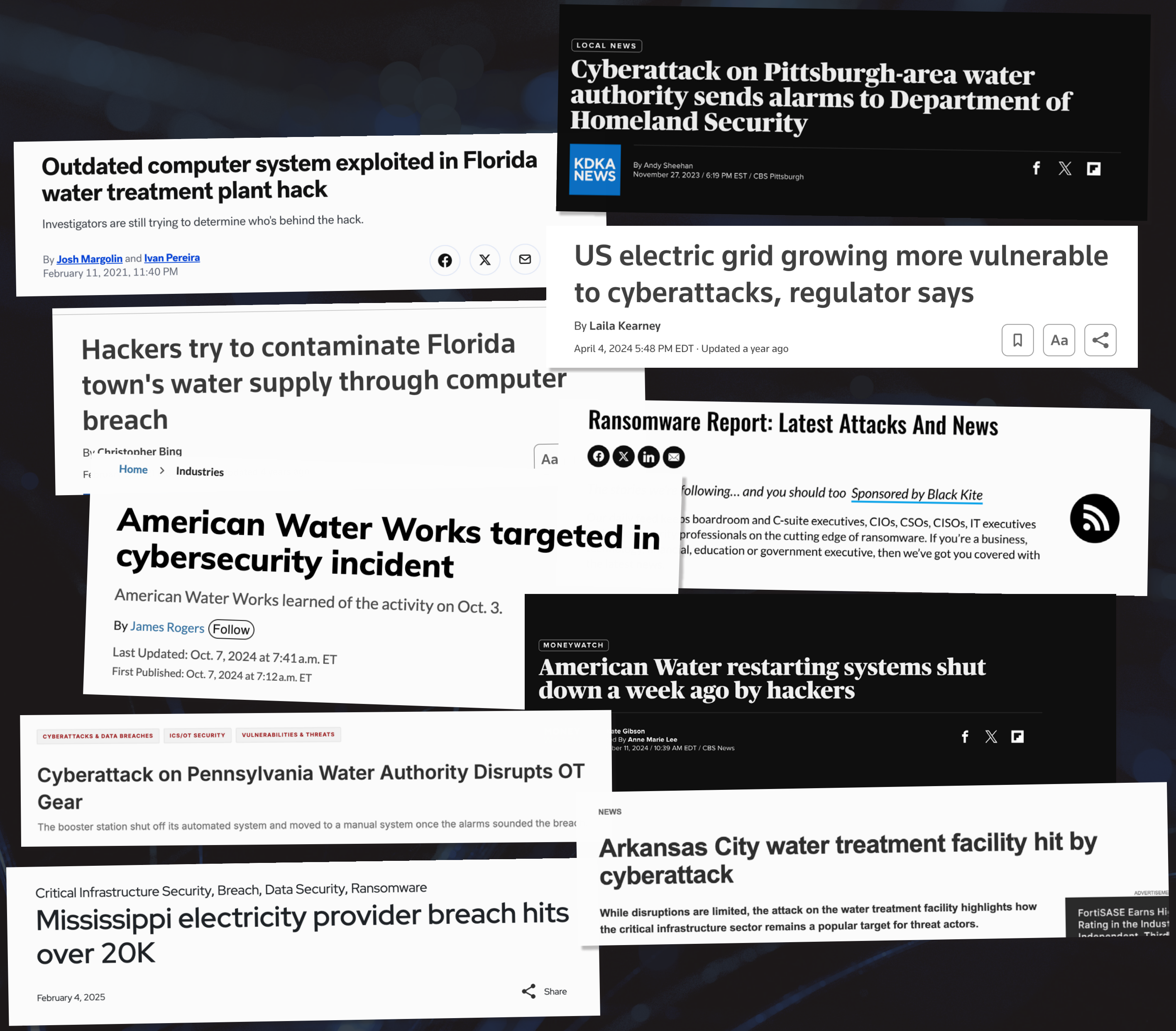


TABLE OF Contents

Increasing Cyberattacks on Utilities

US



LOCAL NEWS

Cyberattack on Pittsburgh-area water authority sends alarms to Department of Homeland Security

KDKA NEWS

By Andy Sheehan
November 27, 2023 / 6:19 PM EST / CBS Pittsburgh

Outdated computer system exploited in Florida water treatment plant hack

Investigators are still trying to determine who's behind the hack.

By Josh Margolin and Ivan Pereira
February 11, 2021, 11:40 PM

US electric grid growing more vulnerable to cyberattacks, regulator says

By Laila Kearney
April 4, 2024 5:48 PM EDT · Updated a year ago

Hackers try to contaminate Florida town's water supply through computer breach

By Christopher Bing

Ransomware Report: Latest Attacks And News

following... and you should too Sponsored by Black Kite

ps boardroom and C-suite executives, CIOs, CSOs, CISOs, IT executives professionals on the cutting edge of ransomware. If you're a business, al, education or government executive, then we've got you covered with

Home > Industries

American Water Works targeted in cybersecurity incident

American Water Works learned of the activity on Oct. 3.

By James Rogers (Follow)

Last Updated: Oct. 7, 2024 at 7:41 a.m. ET
First Published: Oct. 7, 2024 at 7:12 a.m. ET

MONEYWATCH

American Water restarting systems shut down a week ago by hackers

ate Gibson
d By Anne Marie Lee
ber 11, 2024 / 10:39 AM EDT / CBS News

CYBERATTACKS & DATA BREACHES | ICS/OT SECURITY | VULNERABILITIES & THREATS

Cyberattack on Pennsylvania Water Authority Disrupts OT Gear

The booster station shut off its automated system and moved to a manual system once the alarms sounded the breac

NEWS

Arkansas City water treatment facility hit by cyberattack

While disruptions are limited, the attack on the water treatment facility highlights how the critical infrastructure sector remains a popular target for threat actors.

Critical Infrastructure Security, Breach, Data Security, Ransomware

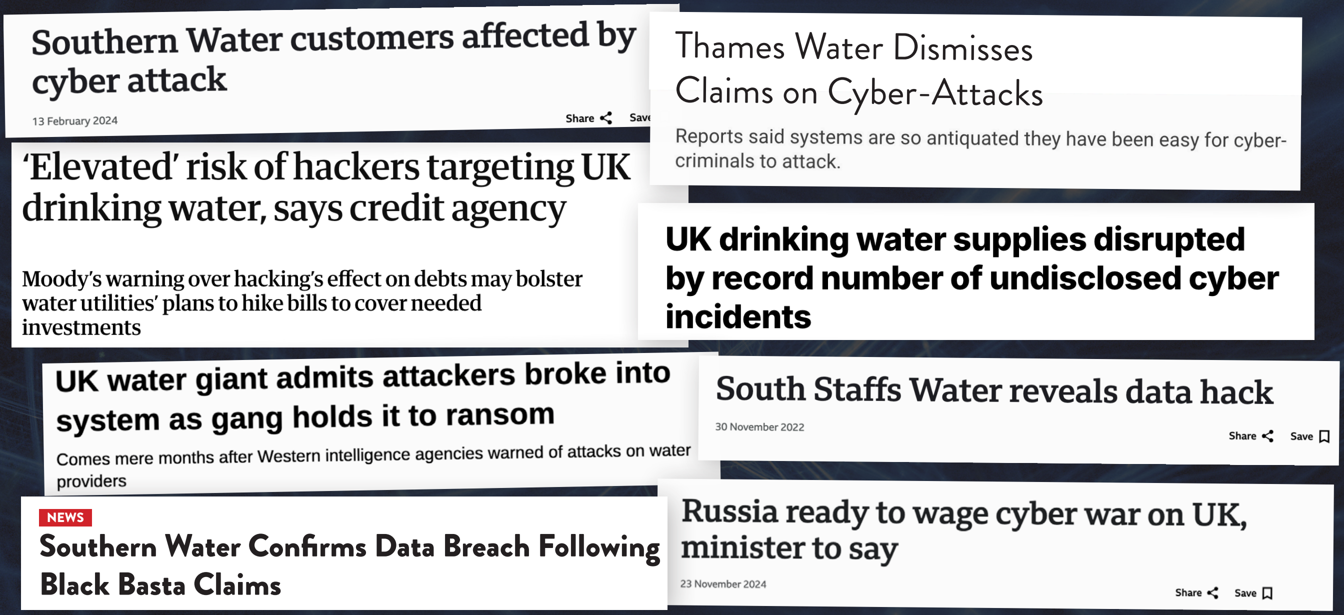
Mississippi electricity provider breach hits over 20K

February 4, 2025

Share

Increasing Cyberattacks on Utilities

UK



Southern Water customers affected by cyber attack

13 February 2024

Share Save

Thames Water Dismisses Claims on Cyber-Attacks

Reports said systems are so antiquated they have been easy for cyber-criminals to attack.

'Elevated' risk of hackers targeting UK drinking water, says credit agency

Moody's warning over hacking's effect on debts may bolster water utilities' plans to hike bills to cover needed investments

UK drinking water supplies disrupted by record number of undisclosed cyber incidents

UK water giant admits attackers broke into system as gang holds it to ransom

Comes mere months after Western intelligence agencies warned of attacks on water providers

South Staffs Water reveals data hack

30 November 2022

Share Save

NEWS

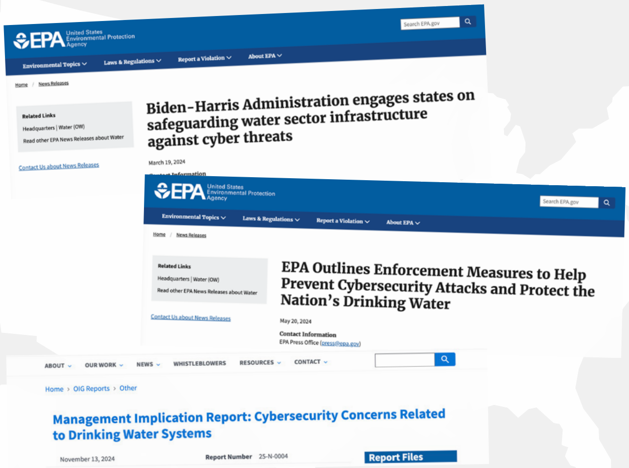
Southern Water Confirms Data Breach Following Black Basta Claims

Russia ready to wage cyber war on UK, minister to say

23 November 2024

Share Save

GOVERNMENT ADVISORIES



EPA United States Environmental Protection Agency
Search EPA.gov
Environmental Topics
Laws & Regulations
Report a Violation
About EPA
Home / News Releases
Related Links
Headquarters | Water (OW)
Read other EPA News Releases about Water
Contact Us about News Releases

Biden-Harris Administration engages states on safeguarding water sector infrastructure against cyber threats

March 19, 2024

EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation's Drinking Water

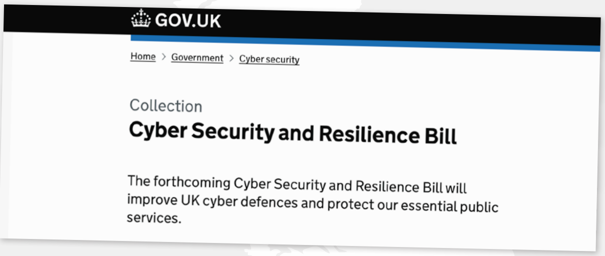
May 20, 2024

Contact Information
EPA Press Office (press@epa.gov)

ABOUT
OUR WORK
NEWS
WHISTLEBLOWERS
RESOURCES
CONTACT
Home › OIG Reports › Other

Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems

November 13, 2024 Report Number 25-N-0004



Collection

Cyber Security and Resilience Bill

The forthcoming Cyber Security and Resilience Bill will improve UK cyber defences and protect our essential public services.

A Critical Moment for Critical Infrastructure

THE HEADLINES PAINT A CONCERNING PICTURE

March 2025: A case study reveals that two years earlier, Littleton Electric Light and Water Departments, a US public power utility, discovered that Volt Typhoon, a Chinese threat actor, had been lurking in the utility's systems undetected for nearly a year.

October 2024: American Water Works — the largest water and wastewater utility in the US, serving an estimated 14 million people in 14 states — detects unauthorized activity in its computer network, disrupting customer service and billing.

March 2024: The US Environmental Protection Agency and the Cybersecurity Infrastructure Security Agency warn US governors about a common vulnerability in water and wastewater digital systems.

January 2024: Officials at Southern Water, serving five counties in southern England, discover that the Black Basta group gained access to the company's network and stole personal information belonging to millions of customers and employees.

November 2023: Pro-Iranian attackers breach the Municipal Water Authority of Aliquippa in Pennsylvania, exploiting Unitronics programmable controllers. The same month, the UK's National Cyber Security Centre warns that "state-aligned actors" have emerged as a "new class of cyber adversary" threatening critical infrastructure.

These are just a few examples of recent cyberattacks and threats against water, wastewater, and electricity operators. Is the number of attacks intensifying and, if so, for what purpose?

To answer these questions and examine trends in the frequency and impact of cyberattacks on both publicly and privately owned water and electricity utilities, Semperis worked with research firm Censuswide to conduct a study of 350 utilities: 250 in the US and 100 in the UK.

Understanding and mitigating the increasing cyber risk for water and electricity utilities is a critical challenge that affects both public safety and private industry. This report aims to provide insights that can help utility operators improve both cyber and operational resilience.

> "Ransomware criminals have a propensity to go after locally and municipally operated critical infrastructure, including water treatment facilities and electricity grids. Frankly, with low IT and security budgets staring at operators, threat actors have the upper hand."

Ciaran Martin, CB
Managing Director, Paladin Capital Group
Founding Chief Executive, National Cyber Security Centre (UK)

Utility Systems Under Threat

“Attackers know that disrupting water treatment facilities or power grids can cause widespread panic and economic damage, increasing the pressure on operators to pay the ransom quickly,” explains Ciaran Martin, CB, Paladin Capital Group Managing Director and founding Chief Executive of the UK’s National Cyber Security Centre.

Our study confirms the importance of an assume-breach mindset for utility operators. Most respondents in our study (**62%**) reported that they had been targeted by threat actors during the past year. Among the utilities that had been attacked, the vast majority (**80%**) were hit multiple times.

Yet the fact that more than one-third (**38%**) of respondents believed that they had not been targeted is even more troubling. According to cybersecurity experts, it’s more likely that a good portion of these utilities simply don’t have the funding or resources to detect attacks that are designed to remain hidden.

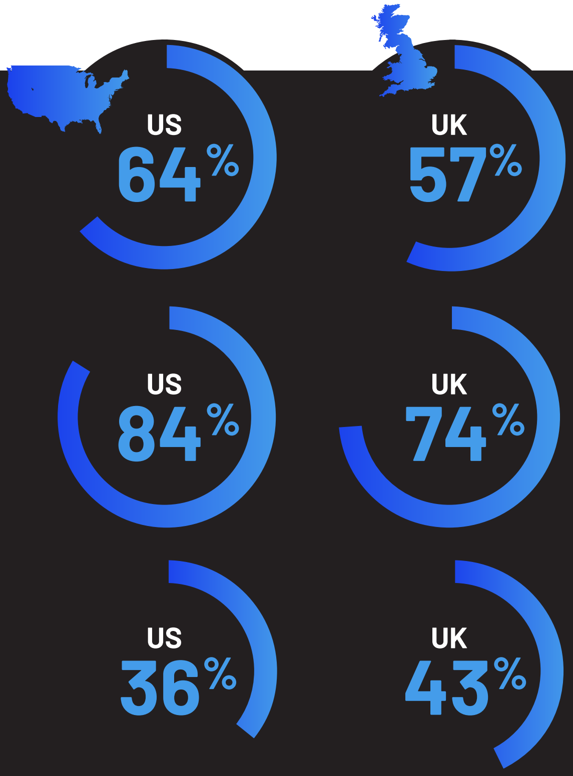
> “Utilities are a prime target for nation-states, probably more than criminal gangs. It’s also not surprising they were attacked multiple times, given that nation-states are well resourced and time is not a constraint.”
>
> **Simon Hodgkinson**
> Former CISO, bp
> Strategic Advisor, Semperis

Who is behind these attacks? More than half (**59%**) of respondents verified that nation-state actors were responsible. Another **14%** were unsure of the attack source.

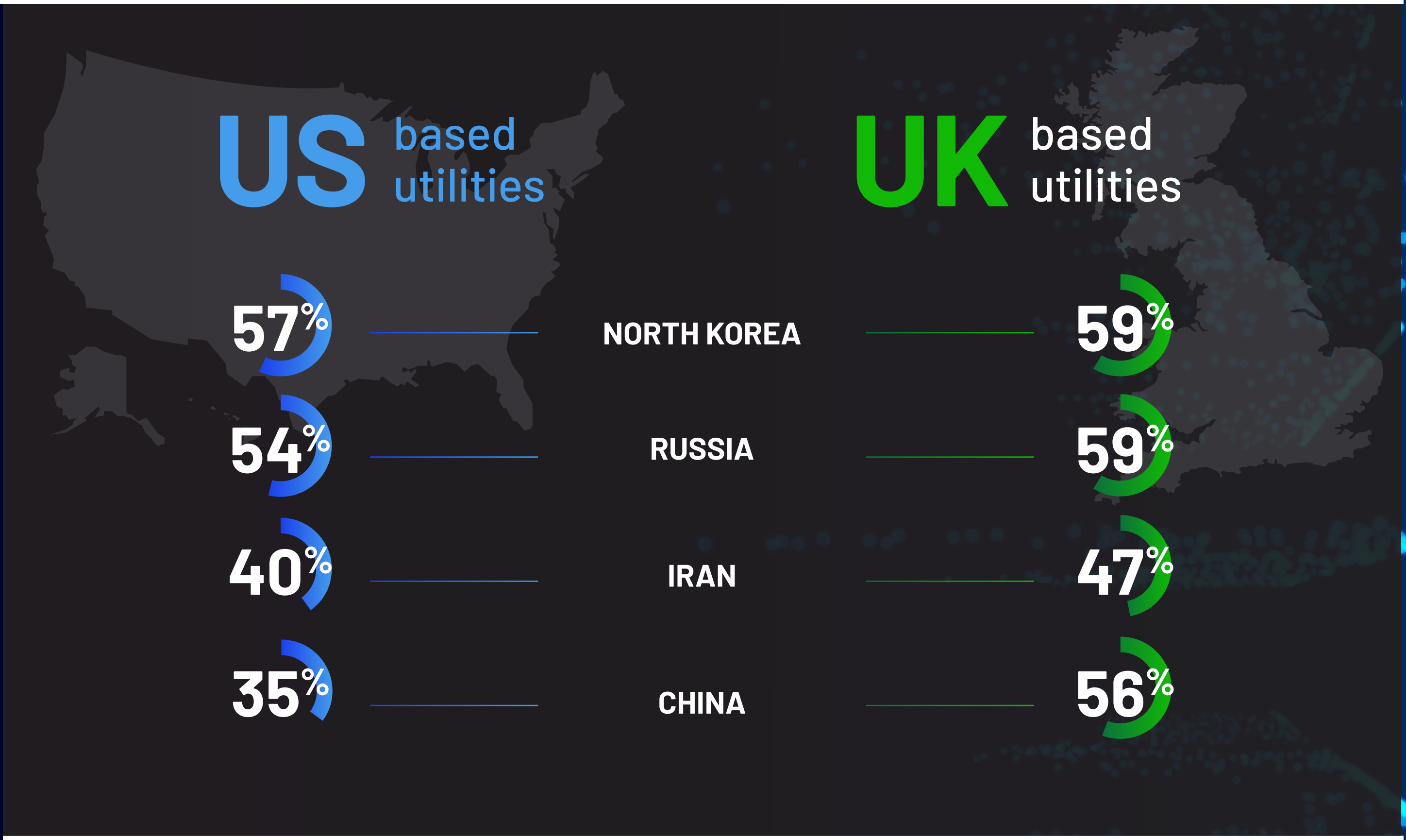
62% reported being targeted by cyberattacks

80% of those were attacked multiple times

38% reported not being targeted



NATION-STATES PERPETRATING ATTACKS ON UTILITIES



US based utilities		UK based utilities
57%	NORTH KOREA	59%
54%	RUSSIA	59%
40%	IRAN	47%
35%	CHINA	56%

According to former bp CISO and Semperis Strategic Advisor Simon Hodgkinson, nation-state threats see infrastructure attacks as opportunities to gain international leverage or support their economies. Cybercrime also tends to increase in line with trade sanctions.

Chris Inglis, former US National Cyber Director and Semperis Strategic Advisor, adds, “Nation-states have increasingly realized that not just the routines of daily life but the engine of commerce and the nation’s confidence depend on digital infrastructure working as expected.”

Inglis believes that the financial motivations of North Korean actors — who are quick to demand ransom — explains why that nation-state dominated the attacks in our survey. Attackers that are motivated by espionage or political leverage are less likely to make themselves known than those that are after a fast payout. He emphasizes that cybercriminals’ appetite for income is also insatiable, so utility operators who have not received ransomware demands should never underestimate the threat against their operations.

“Many public utilities likely don’t realize that China has infiltrated their infrastructure,” Inglis explains. Worse, Chinese-sponsored threat actors like Volt Typhoon are known to prefer *Living off the Land* attacks, which make attackers difficult to detect, especially as they remain dormant for long periods—planting backdoors, gathering information, or waiting to strike for months or even years.

Impacts to Public Infrastructure: Disruption, Corruption, and Theft

The potential public impacts of being without electricity, heat, or clean water for even a short period can be significant. Our study indicates that utility customers in the US and UK have been relatively fortunate — so far. More than half of those who reported attacks experienced disruption of their operations (**57%**); data, IP, or PII theft (**55%**); and even permanent corruption or destruction of data or systems (**54%**). However, most were also able to restore services within 24 hours (**84%**).

> "Embracing an assume-breach mindset is crucial for rapid recovery from cyberattacks. At the same time, implementing identity forensics and incident response (IFIR) capabilities enhances operational resilience, ensuring that identity systems remain secure against evolving threats. In an environment where regulations like DORA, GDPR, and NIST mandate robust identity protection and swift breach response, IFIR provides a proactive, structured framework that helps minimize business disruptions and safeguard critical infrastructure from compromise."
>
> **Simon Hodgkinson**
> Former CISO, bp
> Strategic Advisor, Semperis

Mickey Bresman, CEO of Semperis, suspects this means that the utilities surveyed haven't yet faced a large-scale incident. His assumption is that intruders, especially those affiliated with nation-states, remain dormant, waiting for the right time to cause disruptions.

"Look at the Colonial Pipeline attack," he says, referring to the May 2021 incident in which Russia's DarkSide ransomware gang disrupted the gasoline supply along the US East Coast. "It took the company weeks to fully recover. While they ended up paying $4.4 million in ransom, officials soon realized the decryption keys were corrupted, leaving them no choice but to deploy backup data files. Fortunately, the ransomware group in this case wasn't able to breach OT resources, as the company proactively disconnected those networks."

A recently published case study out of the US describes how Volt Typhoon, a well-known threat actor backed by China, infiltrated a public power utility in Massachusetts. In that instance, the intruders were discovered to have been lurking in the utility's network for nearly a full year. This incident illustrates the potential danger of difficult-to-detect threats and threat-actor persistence.

Hodgkinson believes many of the attacks we've seen on utilities are simply opening salvos, carried out either to gauge the effectiveness of a nation's cybersecurity defenses or to plant backdoors for future attacks. What we're seeing now, he warns, is likely a precursor of future disruption.

To maintain operational resilience, critical infrastructure operators need attack-detection capabilities that provide visibility into both sophisticated and stealthy intrusions. They also need to adopt an assume-breach mindset and prepare to respond to and securely recover from attacks that target and hide in critical parts of the infrastructure.

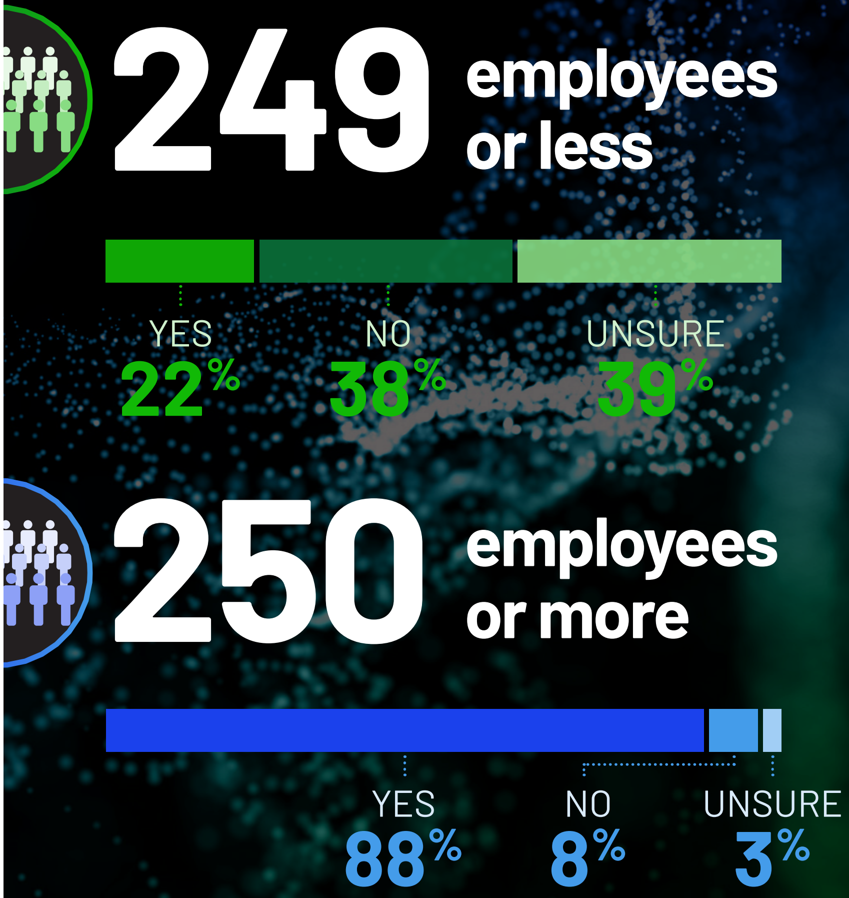
Risks to Operational Resilience

Our study indicates that critical identity systems — Microsoft Active Directory, Entra ID, and Okta — were definitively compromised in **67%** of these attacks, with another **15%** of respondents unsure whether those systems were affected. Interestingly, US utilities were nearly **20%** more likely to see their identity systems breached.

Larger utility operators also reported a much greater likelihood of identity system breaches. Larger organizations naturally have larger identity environments that are more difficult to audit and manage. Plus, smaller operators often lack the capabilities to detect these types of attacks."

[Previous studies](#) conducted by Semperis reveal that too few organizations are prepared for effective hybrid Active Directory recovery. This oversight is a concern for any organization, but especially for those providing critical infrastructure services.

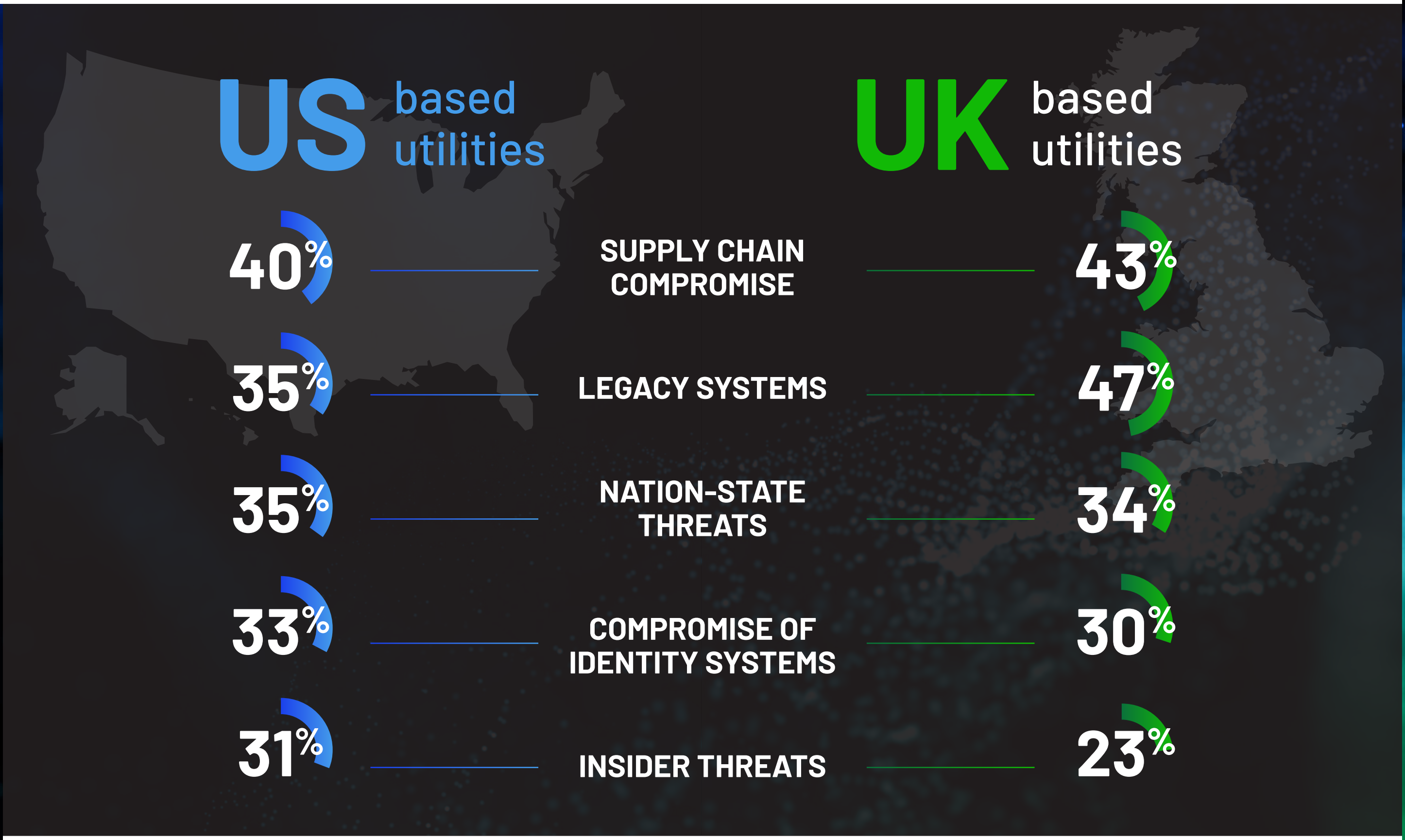
IDENTITY SYSTEMS COMPROMISED IN UTILITY OPERATIONS



> "From post-attack engagements in breached environments, we know that 90 percent of the time, identity systems are targeted and successfully compromised. Unfortunately, many organizations lack the tools needed to gain visibility into those compromises, preventing them from restoring trust in their identity systems."

Mickey Bresman
CEO, Semperis

BIGGEST CYBERSECURITY RISKS



	US based utilities	UK based utilities
SUPPLY CHAIN COMPROMISE	40%	43%
LEGACY SYSTEMS	35%	47%
NATION-STATE THREATS	35%	34%
COMPROMISE OF IDENTITY SYSTEMS	33%	30%
INSIDER THREATS	31%	23%

Tellingly, only about one-third of respondents in this study named identity system compromise as a top cybersecurity risk. However, Active Directory's primary role in most cyberattacks likely makes it a key factor in every other risk that respondents identified.

Identity systems are Tier 0 services that manage access to nearly all users, groups, applications, and resources. Without a functional identity system, users cannot log in and resources cannot be accessed. Attackers also use identity compromise to move laterally and escalate their privileges in the breached environment. Therefore, operational resilience is highly dependent on the ability to quickly and securely recover Active Directory and other identity systems.

A September 2024 report from the Five Eyes Alliance — a cybersecurity advisory group made up of leaders from the US, UK, Canada, Australia, and New Zealand — encouraged organizations to "better protect Active Directory from malicious actors." The report notes that "Active Directory's pivotal role in authentication and authorization makes it a valuable target for malicious actors" and details reasons for the service's susceptibility, including a lack of effective solutions for detecting and diagnosing security vulnerabilities in the identity infrastructure.

"Microsoft's Active Directory is the most widely used authentication and authorization solution in enterprise IT networks globally," according to the advisory, which concluded that Active Directory security is pivotal to "overall network security."

The Age of Resilience

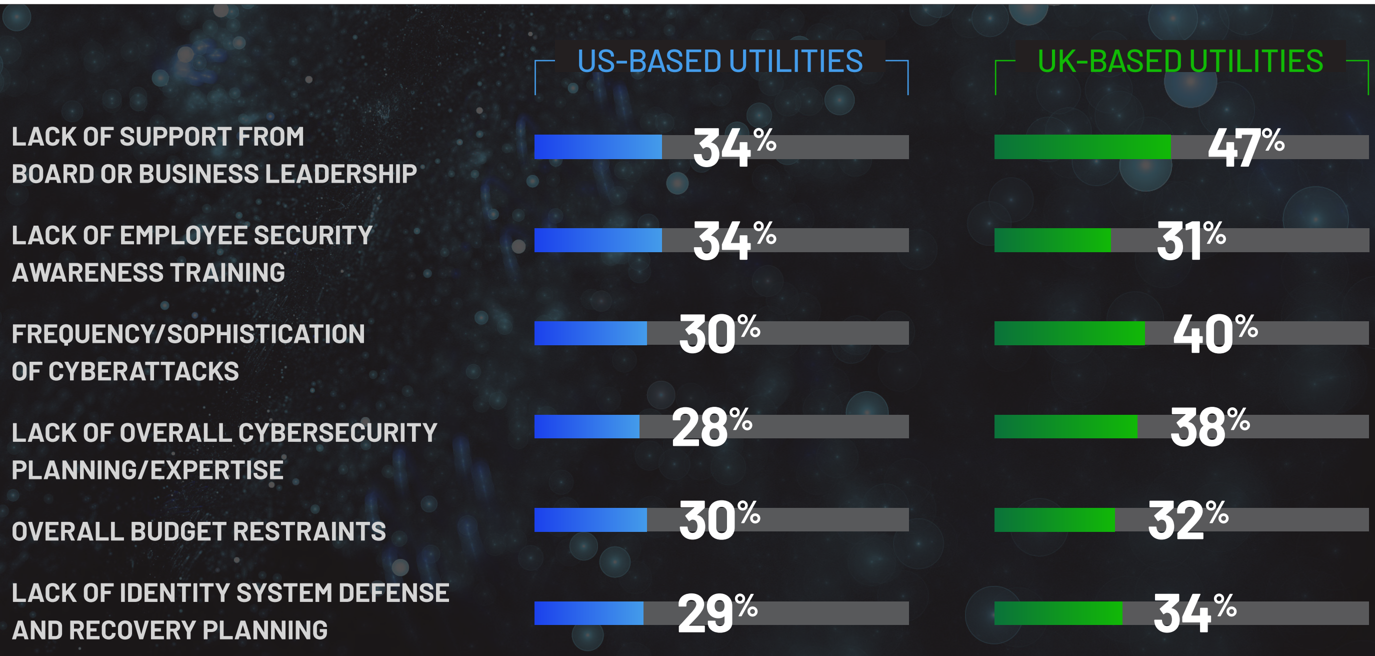
> “Cyber resilience is about people, processes, and the ability to respond in a timely fashion when everything is on the line. Organizations must be prepared to respond swiftly and decisively when cyber threats strike. This involves having an assumed-breach mindset approach to navigate crises effectively, ensuring minimal disruption to business operations.”
>
> **Ciaran Martin, CB**
> Managing Director, Paladin Capital Group
> and Founding Chief Executive, National Cyber Security Centre (UK)

When we asked study participants about the biggest challenges to improving their cyber resilience, we found — unsurprisingly — that several of their answers mirrored those of other industries we've surveyed.

These challenges include a lack of:

- Employee **training** and expertise
- **Budget**
- Board or leadership **support**
- Identity **system defense** and recovery planning

BIGGEST CHALLENGES TO IMPROVING CYBER RESILIENCE IN 2025



What sets utility operators apart from many other industries is the critical nature of their work product. If an electricity or water operator is compromised, the potential risks to public health and safety can put the entire nation at risk. Our experts note that resilience to cyberattacks that threaten operations should be the top priority for every organization involved in critical infrastructure.

This level of preparedness requires utility operators not just to aim for cyber resilience but to adopt a holistic resilience mindset. Today's complex cyber threat landscape demands a proactive approach to resilience — one that assumes breach and readies the organization to respond to and recover from any threat that can interrupt its mission.

"Resilience of utilities' people, processes, and technology should be tested through tabletop exercises, modeling a variety of attack scenarios. Assurance of a proper attack response will be a key factor in the strength of their future cyber and operational resilience," says Bresman.

With a resilience mindset, cybersecurity is no longer simply a cost center under the responsibility of the IT department. It is a mission-critical business unit that requires input and involvement from everyone in the organization.

As Hodgkinson notes, "It starts with leadership. When leadership at an organization takes an interest in improving operational resilience, it will happen, and budgets will be allocated to projects that improve the protection of critical infrastructure."

To become **truly resilient,** organizations should:

1. **Identify Tier 0 infrastructure components** that are essential for recovery from a cyberattack.
2. **Prioritize incident response and recovery** for these systems, followed by mission-critical (Tier 1) functions, business-critical (Tier 2) functions, and then all other (Tier 3) functions.
3. **Document response and recovery processes and practice them** using real-world scenarios that involve people and processes beyond the IT department.
4. **Focus not just on fast recovery but on secure recovery.** Attackers often attempt to compromise backups to maintain persistence in the environment, even after recovery attempts. Implement solutions that support speed, security, and visibility in crisis situations.

"Cyber resilience isn't just about technology — it's about people, processes, and the ability to act decisively when everything is on the line," says Bresman. "Response times to cyberthreats will be faster if organizations assume that adversaries are already in their networks and have a documented and tested recovery and resilience plan that is ready to deploy at a moment's notice."

As suppliers of critical infrastructure services, utility operators — both public and private — can benefit from adopting a resilience mindset that increases their ability to respond to and recover from widespread attacks that threaten the public they serve.

METHODOLOGY

In early 2025, utility operators across the US and UK participated in a detailed study of their experience with cyberattacks and ransomware. To conduct this study, we partnered with experts at Censuswide, an international market research consultancy headquartered in London. Censuswide surveyed 350 water, water treatment, and electricity operators (250 US operators and 100 UK operators).

HOW TO CITE INFORMATION IN THIS REPORT

The data in this report are provided as an information source for the cybersecurity community and the organizations it serves. Semperis encourages you to share our findings. To cite statistics or insights, reference the Semperis *The State of Critical Infrastructure Resilience* report and link to the full report, which is downloadable at https://www.semperis.com/the-state-of-critical-infrastructure-resilience/.

To interview Semperis experts, contact Bill Keeler at billk@semperis.com. Lastly, we'd love to hear your questions or thoughts on the topic of ransomware and resilience. Find Semperis on LinkedIn.

ABOUT SEMPERIS

semperis

+1-703-918-4884 | info@semperis.com | www.semperis.com
5 Marine View Plaza, Suite 102, Hoboken, NJ 07030