

The Threat Is Real: The State of Cybersecurity in Utilities

Critical infrastructure like utilities are prime targets for foreign and domestic threat actors. As utility providers modernize through automation and digitized connections, they open the door to increased cyberattacks — by outside entities or from inside the walls — requiring an updated approach to identity security.

In recent years...

Utilities have been a prime target for cyberattacks:

56%

of utility providers faced cyberattacks¹

Breach notifications in the utilities sector jumped²

400%

Electricity providers in

18

states were attacked³

The consequences of a breach were severe:

The average cost of a utility data breach was

\$6.39 million⁴

It took an average of

205 days

to fix critical vulnerabilities after an incident⁵

15,000

residents were at risk of being poisoned by an attempted hack at a Florida water utility⁶

Identity security is critical to protecting utilities:

30%

of data breaches at utility providers involve internal actors⁷

37%

of utility providers experience **compromised employee credentials**⁸

1

compromised employee password caused the hack that **took down one of the largest** natural gas pipelines in the United States

Areas of opportunity:

The good news is there are three clear strategies utility providers can use to begin creating a smarter approach to identity security:

1

Focus on individual employees' access.

Enterprise-wide security begins with each worker.

2

Eliminate manual processes.

Automation saves time and reduces the risk of error.

3

Stay compliant.

Adopt a strategy for faster adaptation to ever-changing compliance requirements.

Workers are the new perimeter. Identity security is the new firewall. And automation is the key to success.

?

Identity security helps answer three critical questions:

1 | Who has access to what?

2 | Who *should* have access?

3 | How are they *using* their access?

Utility organizations that use SailPoint to automate identity processes can reduce costs, increase visibility and improve compliance and security.



Quickly mobilize your workforce with faster onboarding



Reduce the time and increase the security associated with deprovisioning access



Mitigate the risk associated with contractor, third party and contingent worker access



Help ensure sensitive data and critical applications are accessed by the right people in the right locations



See and control user access to all applications and data – in the cloud, on-premise and in legacy systems – to enable increased security and compliance

Learn more.

See how SailPoint and PwC are helping the utilities industry create more secure, more efficient, more compliant identity security systems.

Download the white paper.



¹ Jaclyn Brandt. "Survey: 56 percent of utilities have faced a cyberattack in the last year." Daily Energy Insider. October 2019.

² "2021 Data Breach Outlook." Kroll.

³ Matthew Stolle. "Cyberattacks Continue Against U.S. Utility Companies." Government Technology. November 2019.

⁴ Rob Robinson. "SOARing Costs? Considering Data Breach Economics." Complex Discovery. March 2021.

⁵ "Survey finds utilities industry has the highest Window of Exposure." Security Magazine. June 2021.

⁶ Jed Pressgrove. "Cybersecurity: The Latest Challenge for Local Water Utilities." Government Technology. March 2021.

⁷ Verizon. "2020 Data Breach Investigations Report."

⁸ SailPoint. "Using Identity and Access Governance to Mitigate Data Breach Risks."

⁹ William Turton and Kartikay Mehrotra. "Hackers breached Colonial Pipeline with one compromised password." Aljazeera. June 2021.