White paper

Securing the Voice Network: An imperative for energy utility companies.

Sarah Simon
Business Development Strategy, Manufacturing | Energy | Utility V3.0
October 12, 2021

Table of contents

Brief Background and Methodology	2
The State of Voice Security in Utilities	3
Utilities Must Do More to Secure Their Voice Networks	3
All Utility Segments at Risk	3
Voice Security in Utilities: Clear and Present Risk	3
How They Do It: The Tricks of the Trade	4
Why the Voice Network is a Target	5
What a Hacker Wants: Money and Power	6
What is at Risk: The Price to Pay for an Unsecured Voice Channel	6
Utility Call to Action: Secure the Voice Network	7
Initial Steps to Establish Voice Security	7
Many Roles in a Utility have a Stake in Voice Security	8
Building the Business Case for Voice Security	8
What Are You Waiting For?	9

verizon✓

Brief Background and Methodology

In June 2021, the author interviewed eight US-based experts in voice security to discuss the challenges and rewards of securing the voice (phone-based) network, specifically the implications of this discipline on companies in the electric, gas and water utility industry. Each professional was asked to delve deeply into the current state of the utility voice security space and share their insights into what actions can be taken to shore up the phone channel defenses.

Fresh in many minds during these discussions was the Colonial Pipeline hacking incident, which rocked the oil and gas transmission space and caused consumer panic, especially in the eastern United States. The paralyzing effect of ramsomware, combined with social media pressure and intense media coverage, resulted in a pipeline with no retail customers to pay millions in dollars in ransom to end the attack.

Utility companies are expected to keep critical resources safe and available. They must guard their physical and IT infrastructures -- and their customers -- from bad actors. Introduced here are the voice security experts interviewed, professionals who have together committed many decades upon decades of career energy to securing business phone systems and call centers.

Exelon
Dale Stone, Senior Systems Engineer, Unified Communications

SecureLogix
Matt Rowan, VP of Channel Development
Bruce Wertman, VP of Engineering

Verizon
Hans Van Arkel, Director Systems Architecture
Pete Tomfohrde, Senior Manager Business Development Strategy Manager
Mark Voorheis, Manager Advanced Communications Products
Shawn McGowan, Voice Security Product
Tony Lesley, Innovation Principal and Utility Lead

The state of voice security in utilities

Utility companies invest in and rely on critical infrastructure. Disruption of the flow of electricity, gas or water services can cripple communities and commerce. Ask anyone who has sat in the dark with no heat/cooling or water for a few days following a major storm, for instance, and they can readily attest to the uncertainty of the situation, and how the problems rippled out to residents and businesses alike in their community. And in an age of social media, utility outages restoration efforts, and community communications are under heightened scrutiny.

Not all utility disruptions are caused by weather events, however. Bad actors can damage essential infrastructure and bring the flow of utility resources to a screeching halt. These bad actors have found creative ways to wreak havoc using the voice networks of utilities companies as a tunnel into their systems. To understand the scope and potential impact of this threat, our security experts were asked to opine on how well utilities perform at protecting their voice infrastructure.

Utilities Can Do More to Secure Their Voice Networks

The consensus among the voice security experts interviewed is that, on average, utility companies could do much more to secure their voice channels. Some companies excel at voice security while others leave the channel dangerously exposed. (Exelon, which contributed to this paper, has a dedicated voice infrastructure security team.)

Why aren't utilities doing more? Reasons given include:

- Utilities are focused first on other aspects of their voice infrastructure, such as scaling to meet peak call volume during weather events.
- There is currently limited regulatory attention on utilities to secure the voice channel.
- The utility industry has been under intense pressure recently, between digital grid, worker safety, carbon reduction demands, M&A consolidation, and divestitures, all of which strain resources, especially IT resources.

Every expert interviewed, however, agrees it is an important mission to help utility companies to improve their voice security grade. Too much is at stake for any utility to leave the security door open on their phone systems.

> **"It's our duty to secure this environment to protect these people."**
>
> – Tony Lesley, Verizon

All Utility Segments at Risk

The experts agreed that voice channel risk is an equal opportunity hazard for all utilities, regardless of category: Public utilities vs co-ops vs. investor-owned; small, medium or large; electric, gas, water or combination. All utilities are valuable, potential targets because they are trusted guardians of lighting and electric power, heating and cooling and water and sewage. No utility is too small to be attacked, and not-for-profit status will not keep any utility off of the bad actors' radar.

Voice Security in Utilities: Clear and Present Risk

Hackers display seemingly infinite creativity when it comes to crafting methods to compromise a utility's systems. If the data is somewhere online, hackers want to get to it and then use their access for personal gain. Most modern telephone systems are online, using VoIP (Voice over Internet Protocol). The voice channel is, therefore, and extension of the broader digital environment. But how do bad actors violate voice network defenses?

How They Do It: The Tricks of the Trade

Table 1: Voice Security Attack Vectors

Utility companies are vulnerable on several points: Their corporate telephone network, their customer contact center and in the wild where bad actors can directly attack utility customers.

Toll Fraud	From SecureLogix: Toll Fraud describes a type of fraud where 1-800 numbers are flooded with bogus calls. Those calls generate revenue for the fraudster who has created a fake telephone company and is now billing your toll call provider for carrier fees for a portion of each call, which results in an unexpectedly large bill for you. Also called International Revenue Share Fraud (IRSF), this fraud type exploits technology to make unauthorized calls to premium numbers, including numbers in parts of the world where tolls are exceptionally high or calls placed to specialty lines. Often involves multiple parties engaged in quiet agreement to perpetuate the activity.
Caller ID Spoofing and Impersonation	Per the FCC (Federal Communications Commission): "Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use neighbor spoofing so it appears that an incoming call is coming from a local number, or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity."
Vishing (Voice Phishing)	Vishing attempts to trick victims into giving up sensitive personal information over the phone. Vishing attacks have high-tech elements: they involve automated voice simulation technology, for instance, or the scammer may use personal information about the victim harvested from earlier cyberattacks to put them at ease. Bad actors often use spoofing to fool the fraud victim into thinking he/she is working with a legitimate entity. Vishing follows a familiar social engineering script: An attacker creates a scenario to prey on human emotions, commonly greed or fear, and convinces the victim to disclose sensitive information, like credit card numbers or passwords. - SecureLogix
TDoS Attack (Call Flooding)	According to SecureLogix, a TDoS (Telephony Denial of Service) attack is an attempt to make a telephone system unavailable to the intended user(s) by preventing incoming and / or outgoing calls. The objective is to keep the distraction calls active for as long as possible to overwhelm the victim's telephone system, which may delay or block legitimate calls for service. These attacks can occur unannounced, or proceeded by an extortion threat / random demand.
Fraudulent Robocalls, Spam and Harassing Callers	Refers to a broad class of unwanted, nuisance and malicious calls, which include automated telemarketing/ voice SPAM, and harassing calls.
IVR Data Mining	Taking advantage of customer service automation like IVR (interactive voice response) solutions, hackers pry out sensitive information about your customer service processes in order to gain access to the sensitive information of your customers, simply by silently navigating your IVR prompts.
Eavesdropping	Eavesdropping attacks happen when attackers listen in to voice network traffic. They use unauthorized access to your voice networks so that they may obtain access to data and other sensitive, valuable information.

The Federal Trade Commission warns consumers about fraudulent calls spoofing the identity of utility companies.

Utility company calling? Don't fall for it!

If you get a call from someone claiming to be your utility company, here are some things you can do:

- Thank the caller for the information. Then firmly tell them you will contact the utility company directly using the number on your bill or on the company's website.
- Even if the caller insists you have a past due bill or your services will be shut off, never give banking information over the phone unless you place the call to a number you know is legitimate.
- Utility companies don't demand banking information by email or phone. And they won't force you to pay by phone as your only option.
- If the caller demands payment by gift card, cash reload card, wiring money or cryptocurrency, it is a scam. Legitimate companies don't demand payment by gift cards (like iTunes or Amazon), cash reload cards (like MoneyPak, Vanilla, or Reloadit), or cryptocurrency (like Bitcoin).
- Tell your friends and loved ones about the scam so they can protect themselves. If you got this scam call, others in your community probably did to. We know when people hear about scams, they're much more likely to avoid them.

July 14, 2020

Jim Kreidler

Consumer Education Specialist, FTC

Source: https://www.consumer.ftc.gov/blog/2020/07/utility-company-calling-dont-fall-it

> **"In some cases, millions of calls have been launched into enterprise DID (Direct-Inward Dial) ranges and Toll Free services."**
>
> – Matt Rowan, SecureLogix

Why the Voice Network is a Target

Utility contact center management has worked hard to innovate a modern customer experience to include automation and self-service features. Unfortunately, these enhancements have inadvertently created vulnerabilities for bad actors to exploit. IVR Data Mining is a textbook example of this, where fraudsters navigate utility IVR systems to mine clues that will take them further into data network endpoints, where valuable information can be accessed.

The voice channel is especially vulnerable due to the presence of the human element. Telephony involves people, and social engineers are masters at exploiting human emotion. Take the contact center, for instance. Agents are often hired for their pleasant disposition, and good manners are rewarded. "A contact center agent, their total goal is to be helpful. You can train hard on security issues, but they don't want to mistakenly be too tough on customers", explains Bruce Wertman, VP of Engineering at SecureLogix.

> **Often the weakest link is the human element, and fraudsters recognize this.**
>
> – Matt Rowan, SecureLogix

Bad actors have seen firsthand the improvements many utilities have made toward hardening their digital environment. Over time it has become increasingly more difficult to disrupt utility operations via DDOS attacks or to exfiltrate customer data. However, the voice channel offers a new attack vector and may not be as vigorously guarded as the data channels. According to Tony Lesley, Innovation Principal and Utility Lead at Verizon, "The voice channel often is not well-defended. It's not as protected as other infrastructure." In fact, increased security for data networks has essentially pushed hackers onto the path of least resistance, the voice channel. As explained by Matt Rowan, VP of Channel Development at SecureLogix, "Websites and data networks have been substantially hardened over the past couple of decades, making it more difficult to achieve the desired results by attacking compute infrastructure." Thus, criminals are attacking telephony systems simply because it is easier for them to succeed in the voice environment.

The return on investment (ROI) on voice channel crime is attractive to bad actors, too. Shawn McGowan, Voice Security Product Manager, Verizon, explains: “Some voice fraud has become so cheap and easy. Buy a voice phone line and write a script to automate calls; it’s not expensive, it’s not sophisticated. And there’s a lot of money to be made in fraud, unfortunately. It’s a very profitable business.”

> **Leaving your voice network unprotected is like locking all your doors but leaving a window open to your house.**
>
> – Mark Voorheis, Product Management, Verizon

What a Hacker Wants: Money and Power

Voice system breaches are fairly unsophisticated affairs that yield attractive profits or create leverage for the criminal over the target organization. The opportunity to make money, terrorize a population or twist the arm of a foe are among the motives of cybercrimes against utilities. And because utilities service tens of thousands or even millions of households and businesses, the data they hold is invaluable to identity thieves. All of this means that utilities are high-value, high-profile targets. Here are some examples of voice fraud, driven by the desire to exploit utility companies for income or political leverage.

> **There is always a need to stay ahead of the curve – it is way too profitable to expect the bad actors to just walk away.**
>
> – Shawn McGowan, Product Manager, Verizon

What is at Risk: The Price to Pay for an Unsecured Voice Channel

There is a lot at stake when a voice system is compromised. Beyond managing through the initial chaos engulfing the operations of a compromised entity, there are other concerns to keep in mind. These can include a paralyzed infrastructure, dangers to customer health and safety, revenue loss and other financial costs, the damage to the utility’s brand identity, negative public relations and the burden of increased regulatory scrutiny.

Brand Image	**Financial Cost**
Public Relations	**Customer Trust**
Infrastructure Paralized	**Staff Burnout**
Regulatory Scrutiny	**Revenue Loss**
Health and Saftey	**Operational Disruption**

> **If you make it to the headlines of the national news, your reputation is at stake. It’s a big deal.**
>
> – Bruce Wertman, VP of Engineering, SecureLogix

Utility Call to Action: Secure the Voice Network

“Every company needs a voice firewall” according to Bruce Wertman, VP of Engineering, Secure Logix. This urgency is reinforced by Mark Voorheis, Product Manager, Verizon, who explains: “Voice security is not something extra or special, voice security is part of a comprehensive digital security strategy. Ask yourself: ‘How does this fit in my broader info security picture?’”

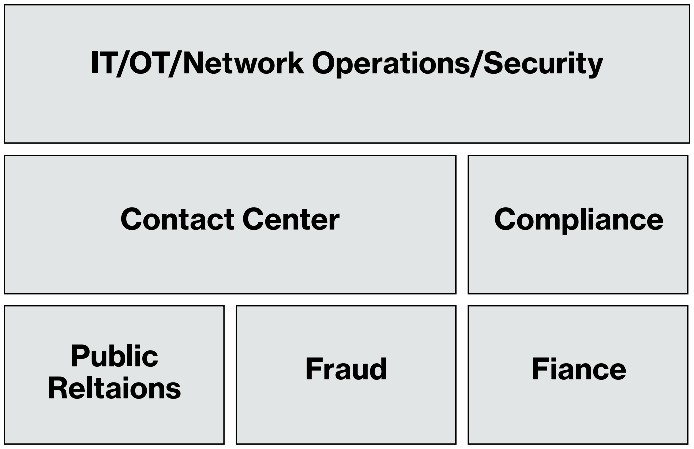
Initials Steps to Establish Voice Security

Having explored the real and persistent threats to utilities, we now explore the remedies. Best practices, technologies and services exist to help your voice system stay safe. Here are some actions leaders in utility companies can take:

- □ Contact the company’s voice carrier for support and to arrange a voice network architecture and voice traffic assessment, including detailed gap analysis and vulnerability assessment
- □ Determine the biggest risk of fraud traffic to the organization (e.g. enterprise telephony or contact center)
- □ Trace the workflow of fraud reports from customers and employees to determine where these reports sit and how the findings are leveraged
- □ Engage the company’s cyber security and risk management teams so that voice security is addressed; align voice security with other security and granted balanced countermeasures
- □ Implement a voice firewall to filter out known bad actors
- □ Educate employees, especially the front line, to understand and spot social engineering
- □ Run penetration tests regularly to identify and respond to evolving voice network threats

Many Roles in a Utility have a Stake in Voice Security

Many stakeholders in a utility have an vested interest in protecting the voice infrastructure. The voice networking teams, security teams and contact center infrastructure teams must seamlessly align for voice system security, preventing bad actors from exploiting gaps between the individual teams and their spans of control. Each of these teams are core contributors toward building and maintaining secure voice networks but other business units also have a vested interest in avoiding a voice breach. Neither the Contact Center leader nor the Public Relations team wants to manage the fallout of a security incident alone. Engage Compliance, Risk and Fraud, and the Finance teams. Leverage these business units as allies in any efforts to harden the voice network security.



Building the Business Case for Voice Security

The security experts interviewed for this paper noted that once a utility company realizes its voice channel security is not all it could be, they then find they are unable to fund the investment to protect the voice infrastructure alone. How do stakeholders and business-line leaders convince the budget decision-makers that the voice security investment must be made? After all, security suffers from a misperception of being purely a cost when in fact it can drive revenue and growth by supporting a more secure and consistent customer experience. Collaboration is the key to influencing the decision-makers.

Voice network carriers (like Verizon) routinely help utility companies document investment justifications, helping quantify the ROI of investing in a more secure voice channel. By inviting the carrier to run a detailed voice security assessment, the resulting documentation will include detailed findings based on an evaluation of the utility's unique environment. A simple analysis of a segment of recent, historic telephony volume can both illustrate and quantify the flow of illicit voice traffic through your network so that the issue can be addressed.

> **"It's not 'if' you get attacked it's 'when'. 'It won't happen to me' or 'I'm willing to take the risk' are not security plans, they're coping mechanisms."**
>
> – Bruce Wertman, SecureLogix

Utility companies not yet ready to work with their carrier in this capacity can do their own voice data breach research search, selecting three to five pertinent stories to educate and inform those guarding the budget. (Tip: Carriers likely can help identify, isolate and communicate these cases!) Bear in mind that the costs of a voice network hack are not limited to financial expense. As Shawn McGowan of Verizon says: "Frontline agents are frustrated by unlawful robocalling and fraud. Customers are frustrated by spoofing calls and social engineering. Reduced compliance from public utility commissioners can become a problem. A lot is at stake."

> **These voice security solutions are not really expensive versus the cost of a breach.**
>
> – Mark Voorheis, Product Management, Verizon

What Are You Waiting For?

Cyber criminals and fraudsters will exploit any weakness they can find. Utility companies, rich in data and providing critical services to the public, are prime targets for voice security attacks. If you think your utility has room for improvement in protecting its voice channel, read Verizon's DBIR (Data Breach Investigation Report) -- and then contact your account representative to begin the journey of bolstering your voice security.

Utility companies not yet ready to work with their carrier in this capacity can do their own voice data breach research search, selecting three to five pertinent stories to educate and inform those guarding the budget. (Tip: Carriers likely can help identify, isolate and communicate these cases!) Bear in mind that the costs of a voice network hack are not limited to financial expense.

As Shawn McGowan of Verizon says: "Frontline agents are frustrated by unlawful robocalling and fraud. Customers are frustrated by spoofing calls and social engineering. Reduced compliance from public utility commissioners can become a problem. A lot is at stake."

Understanding faud tactics

Download Verizon's DBIR
(Data Breach Investigation Report
HERE.

Building a strong voice security strategy

Is your Voice Security Strategy as good as your Data Security Strategy?

Watch this on-demand webinar
HERE.

For more information on Verizon Voice Security offerings visit: www.verizon.com/business/products/contact-center-cx-solutions/voice-security/