JULY 2024

WEBINAR

Voice Security In Healthcare

Understanding a Critical Threat to **Patients**, **Care Givers** & **Access to Quality Care**

mutare

mutare

Agenda

THE STATE OF
VOICE CYBERSECURITY
IN HEALTHCARE

1. Voice Security Terminology & Principles
2. Implications of Inadequate Voice Security
3. How to Eliminate Voice-Based Threats & Strengthen Security Posture

mutare

Presenters

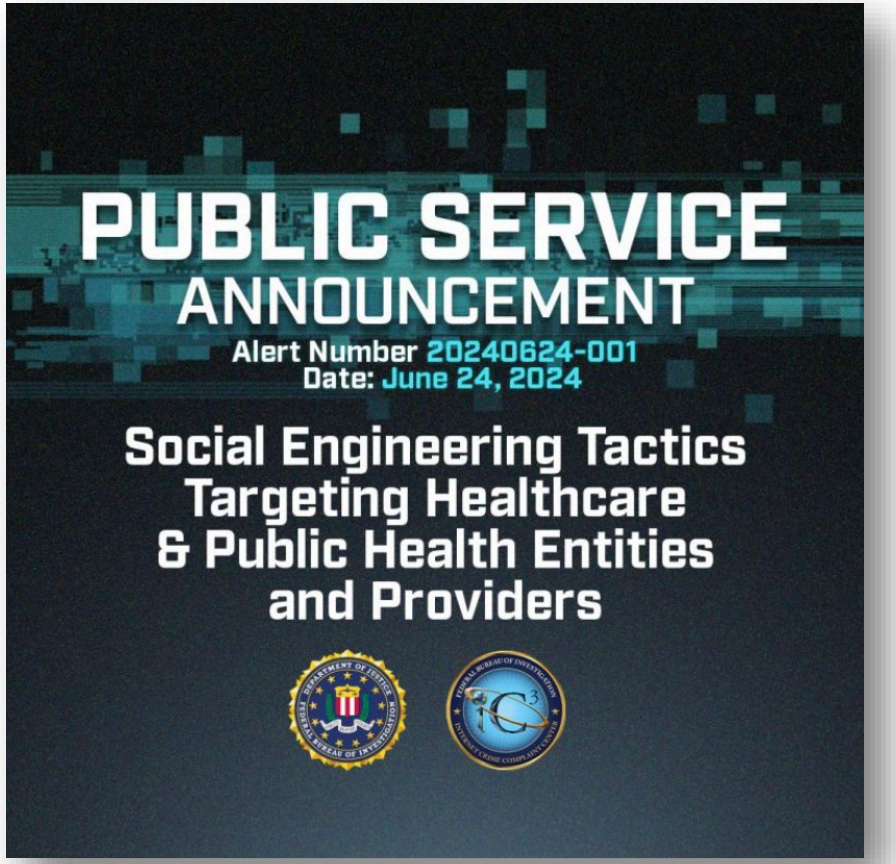
Chuck French

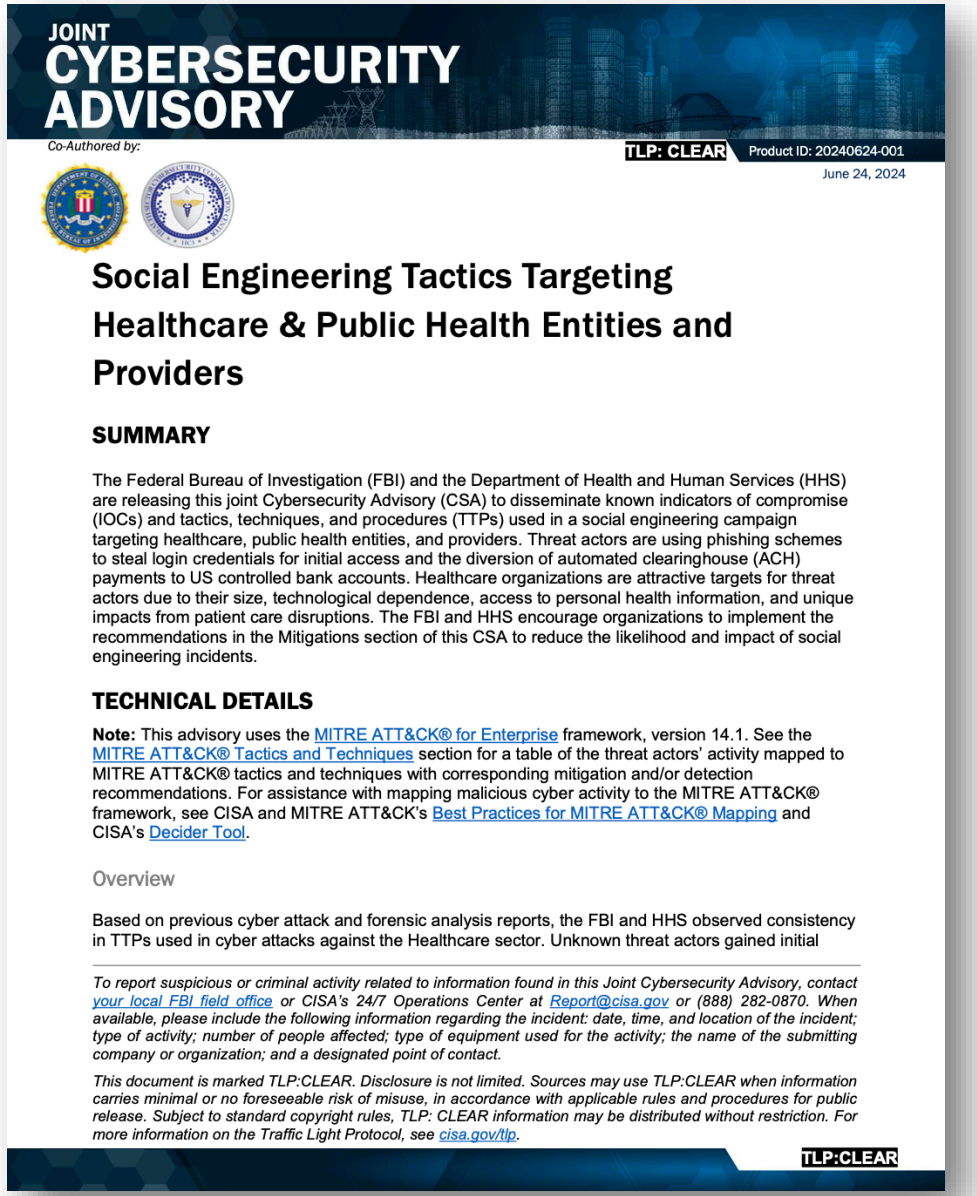
Chief Growth Officer

Vicki Sidor

VP, Sales & Channel

Voice Threats are Real





JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP: CLEAR Product ID: 20240624-001

June 24, 2024

Social Engineering Tactics Targeting Healthcare & Public Health Entities and Providers

SUMMARY

The Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS) are releasing this joint Cybersecurity Advisory (CSA) to disseminate known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used in a social engineering campaign targeting healthcare, public health entities, and providers. Threat actors are using phishing schemes to steal login credentials for initial access and the diversion of automated clearinghouse (ACH) payments to US controlled bank accounts. Healthcare organizations are attractive targets for threat actors due to their size, technological dependence, access to personal health information, and unique impacts from patient care disruptions. The FBI and HHS encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of social engineering incidents.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14.1. See the MITRE ATT&CK® Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques with corresponding mitigation and/or detection recommendations. For assistance with mapping malicious cyber activity to the MITRE ATT&CK® framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK® Mapping and CISA's Decider Tool.

Overview

Based on previous cyber attack and forensic analysis reports, the FBI and HHS observed consistency in TTPs used in cyber attacks against the Healthcare sector. Unknown threat actors gained initial

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

mutare

Voice is an Entry Point for Initial Access

"To gain initial access to victim networks, the threat actor acquired credentials through social engineering or phishing. In some observed instances, the threat actor called an organization's IT Help Desk posing as an employee of the organization, and triggered a password reset for the targeted employee's organizational account [T1566.004]. In some instances, by manipulating the IT Help Desk employees, the threat actor was able to bypass multifactor authentication (MFA) [T1556.006]."

MITRE ATT&CK® TACTICS AND TECHNIQUES

See Tables 2 through 6 for all referenced threat actor tactics and techniques in this advisory.

Table 2: Initial Access

Technique Title	ID	Use
Phishing: Spearphishing Voice	T1566.004	Threat actor uses voice communications to ultimately gain access to victim systems. Spearphishing voice employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications.

mutare

Initial Access → The Change Healthcare Breach

AHA's Survey re Impact of Change Breach

SURVEY TO ALL U.S. HOSPITALS

The American Hospital Association fielded a survey to all U.S. hospitals on the impact of the Change Healthcare cyberattack The following results represent responses from nearly 1,000 hospitals and were collected between Friday, March 9, 2024 and Tuesday, March 12, 2024.

AHA Survey

Change Healthcare Cyberattack Having Significant Disruptions on Patient Care, Hospitals' Finances

74% of hospitals report direct patient care impact.

94% of hospitals report financial impact, with more than half reporting "significant or serious" impact.

Most hospitals are implementing workarounds, but they are labor intensive and costly.

https://www.aha.org/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances

SURVEY FINDINGS

74% of Hospitals

report direct patient care impact

Nearly 40%

report patients having difficulty accessing care because of delays in processing of health plan utilization requirements (e.g. prior authorization).

94% of Hospitals

report financial impact, with more than half reporting "significant or serious" impact

mutare

From HHS (U.S. Department of Health and Human Services)

Cybersecurity in Healthcare

HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors

Cyber incidents affecting hospitals and health systems have led to extended care disruptions, patient diversions to other facilities, and delayed medical procedures, all putting patient safety at risk.

U.S. Department of Health and Human Services
Enhancing the health and well-being of all Americans

CYBER INCIDENTS RISING

93% Increase
in large breaches reported

278% Increase
in large breaches involving ransomware

https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html

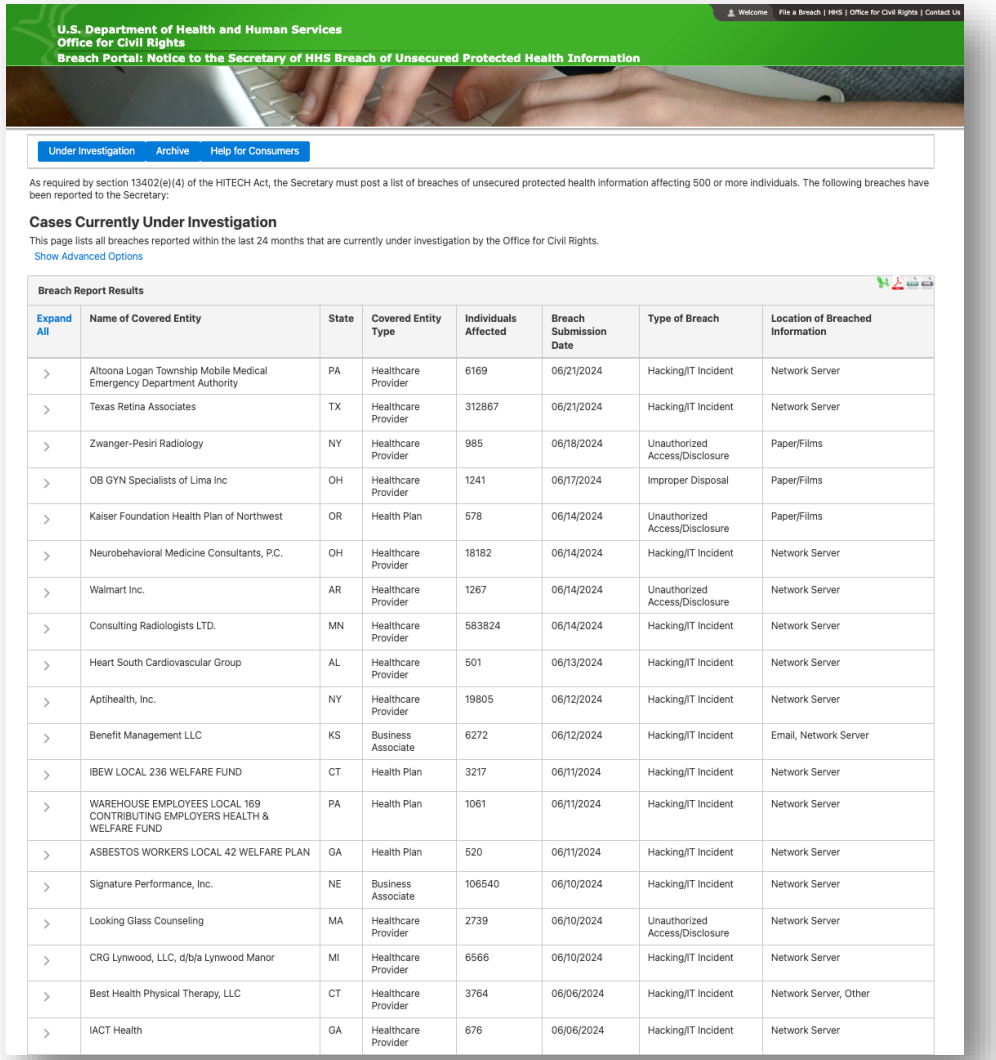
mutare

The Breadth of Breaches is Astounding

As required by section 13402(e)(4) of the HITECH Act, the Secretary of the The U.S. Department of Health and Human Services Office for Civil Rights must post a list of breaches of unsecured protected health information affecting 500 or more individuals.

In the last two years, there are almost 900 cases under investigation.

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf



U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Welcome | File a Breach | HHS | Office for Civil Rights | Contact Us

Under Investigation | Archive | Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

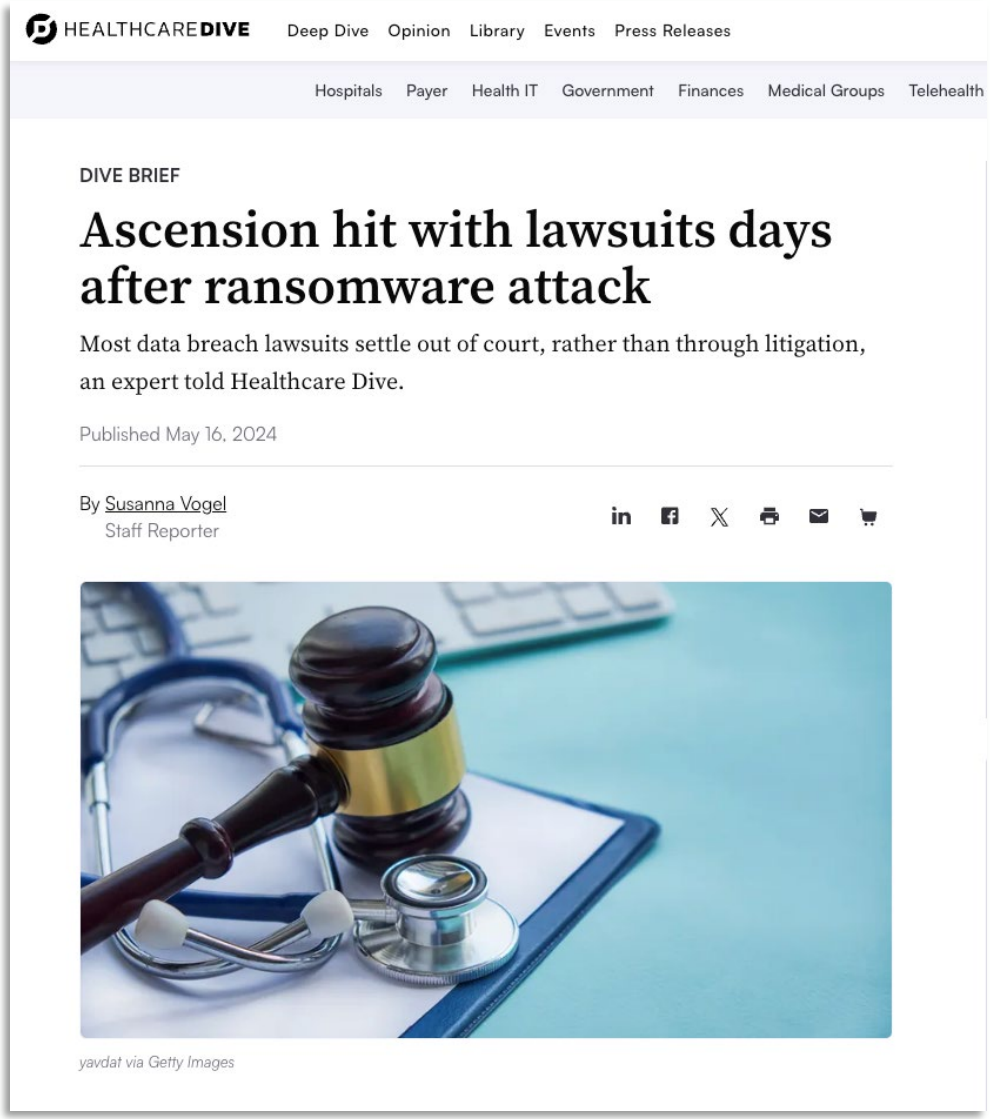
Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
>	Altoona Logan Township Mobile Medical Emergency Department Authority	PA	Healthcare Provider	6169	06/21/2024	Hacking/IT Incident	Network Server
>	Texas Retina Associates	TX	Healthcare Provider	312867	06/21/2024	Hacking/IT Incident	Network Server
>	Zwanger-Pesiri Radiology	NY	Healthcare Provider	985	06/18/2024	Unauthorized Access/Disclosure	Paper/Films
>	OB GYN Specialists of Lima Inc	OH	Healthcare Provider	1241	06/17/2024	Improper Disposal	Paper/Films
>	Kaiser Foundation Health Plan of Northwest	OR	Health Plan	578	06/14/2024	Unauthorized Access/Disclosure	Paper/Films
>	Neurobehavioral Medicine Consultants, P.C.	OH	Healthcare Provider	18182	06/14/2024	Hacking/IT Incident	Network Server
>	Walmart Inc.	AR	Healthcare Provider	1267	06/14/2024	Unauthorized Access/Disclosure	Network Server
>	Consulting Radiologists LTD.	MN	Healthcare Provider	583824	06/14/2024	Hacking/IT Incident	Network Server
>	Heart South Cardiovascular Group	AL	Healthcare Provider	501	06/13/2024	Hacking/IT Incident	Network Server
>	Aptihealth, Inc.	NY	Healthcare Provider	19805	06/12/2024	Hacking/IT Incident	Network Server
>	Benefit Management LLC	KS	Business Associate	6272	06/12/2024	Hacking/IT Incident	Email, Network Server
>	IBEW LOCAL 236 WELFARE FUND	CT	Health Plan	3217	06/11/2024	Hacking/IT Incident	Network Server
>	WAREHOUSE EMPLOYEES LOCAL 169 CONTRIBUTING EMPLOYERS HEALTH & WELFARE FUND	PA	Health Plan	1061	06/11/2024	Hacking/IT Incident	Network Server
>	ASBESTOS WORKERS LOCAL 42 WELFARE PLAN	GA	Health Plan	520	06/11/2024	Hacking/IT Incident	Network Server
>	Signature Performance, Inc.	NE	Business Associate	106540	06/10/2024	Hacking/IT Incident	Network Server
>	Looking Glass Counseling	MA	Healthcare Provider	2739	06/10/2024	Unauthorized Access/Disclosure	Network Server
>	CRG Lynwood, LLC, d/b/a Lynwood Manor	MI	Healthcare Provider	6566	06/10/2024	Hacking/IT Incident	Network Server
>	Best Health Physical Therapy, LLC	CT	Healthcare Provider	3764	06/06/2024	Hacking/IT Incident	Network Server, Other
>	IACT Health	GA	Healthcare Provider	676	06/06/2024	Hacking/IT Incident	Network Server

mutare

“Reasonable Protection” and Class Action Lawsuits



HEALTHCAREDIVE Deep Dive Opinion Library Events Press Releases

Hospitals Payer Health IT Government Finances Medical Groups Telehealth

DIVE BRIEF

Ascension hit with lawsuits days after ransomware attack

Most data breach lawsuits settle out of court, rather than through litigation, an expert told Healthcare Dive.

Published May 16, 2024

By Susanna Vogel
Staff Reporter

yavdat via Getty Images

“Regardless of how the actual hack is carried out, the language contained in ensuing class action suits consistently points to negligence based on ***failure to take “reasonable” measures*** to protect customer data, a term liberally used by the Federal Trade Commission when prosecuting companies for mishandling protected data.”

https://www.mutare.com/mgm-caesars-lawsuits-elevate-critical-need-for-reasonable-voice-channel-cyber-defense/

mutare

1

Voice Security Terminology & Principles

HEALTHCARE

mutare

Top Attack Types Targeting Voice

ROBOCALLS
NUISANCE / NEFARIOUS

SPOOF CALLS
NEFARIOUS

VOICE SPAM
NUISANCE / NEFARIOUS

VISHING
NEFARIOUS

VOICE SPAM STORMS
NEFARIOUS

SOCIAL ENGINEERING
NEFARIOUS

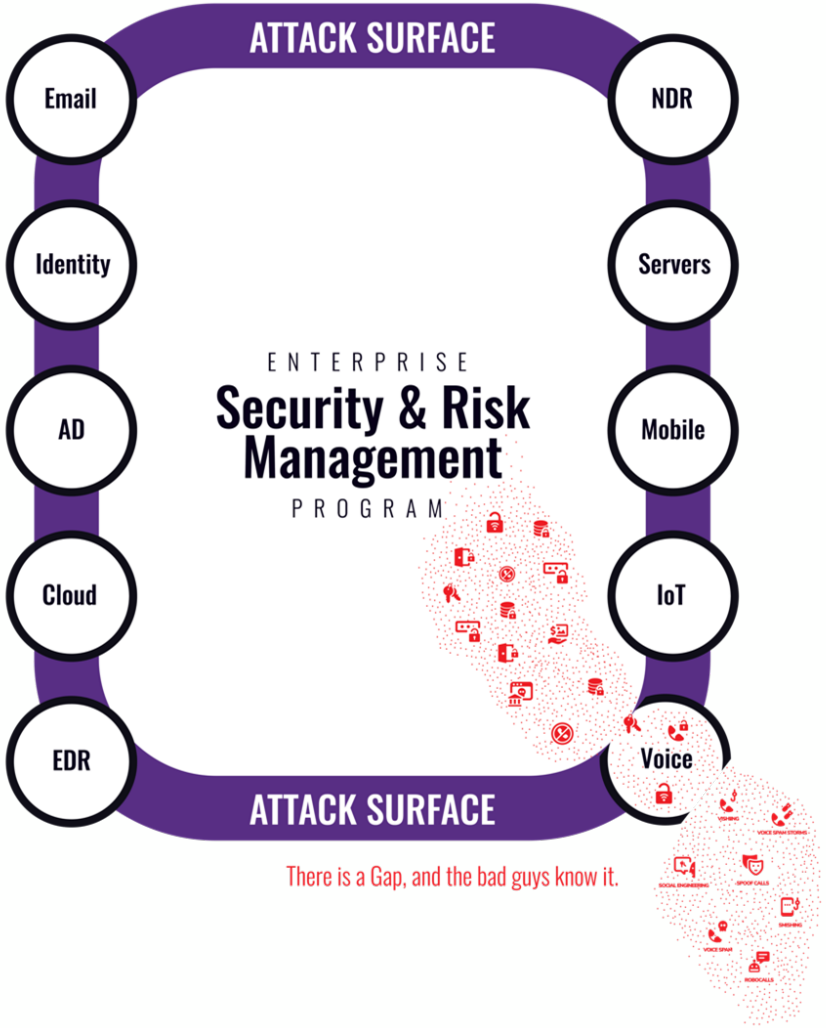
GEN AI
NEFARIOUS

← RAPIDLY EVOLVING

11

The State of Voice Security

- Lack of Awareness of the Risks
- Recommended Solutions are Inadequate
- Telephone Carriers Aren't Solving the Problem
- Voice Security Doesn't Have a Clear Category
- Voice Security Responsibility Varies in Organizations



2

mutare

Implications of Inadequate Voice Security

HEALTHCARE

Healthcare Sector

A Target for Voice-Based Attacks

The critical nature of health-related calls combined with a high-stress environment and duty to respond to every call makes the healthcare sector a uniquely vulnerable flashpoint for voice-based attacks.

Key Impact Zones

- Patient Care
- Patient Experience
- Risk Mgmt & Security

Key Impact Zones

A Flashpoint for Voice-Based Attacks

Patient Care

Voice-based attacks divert institutional attention away from patients, encumber care providers, and reduce care coordination. All of these diminish the organization's ability to deliver a high quality of care.

These realities have the potential to significantly impact patient care and increase the likelihood of Adverse Events.

Patient Experience

Voice-based attacks dramatically impact the Patient Experience as the care journey is dependent on convenient, accessible, secure and timely interactions and communications.

Compromised communications result in diminished care, reduced trust, disrupted information flow, unresponsiveness, increased costs, increased patient vulnerability, and increased susceptibility to fraud.

Risk Mgmt / Security

Voice-based attacks put the institution at risk in multiple categories, most notably: financial, reputational, and operational.

Voice is part of every organization's critical infrastructure which must be covered in their Cyber Defense Strategy & Risk Management Programs.

3

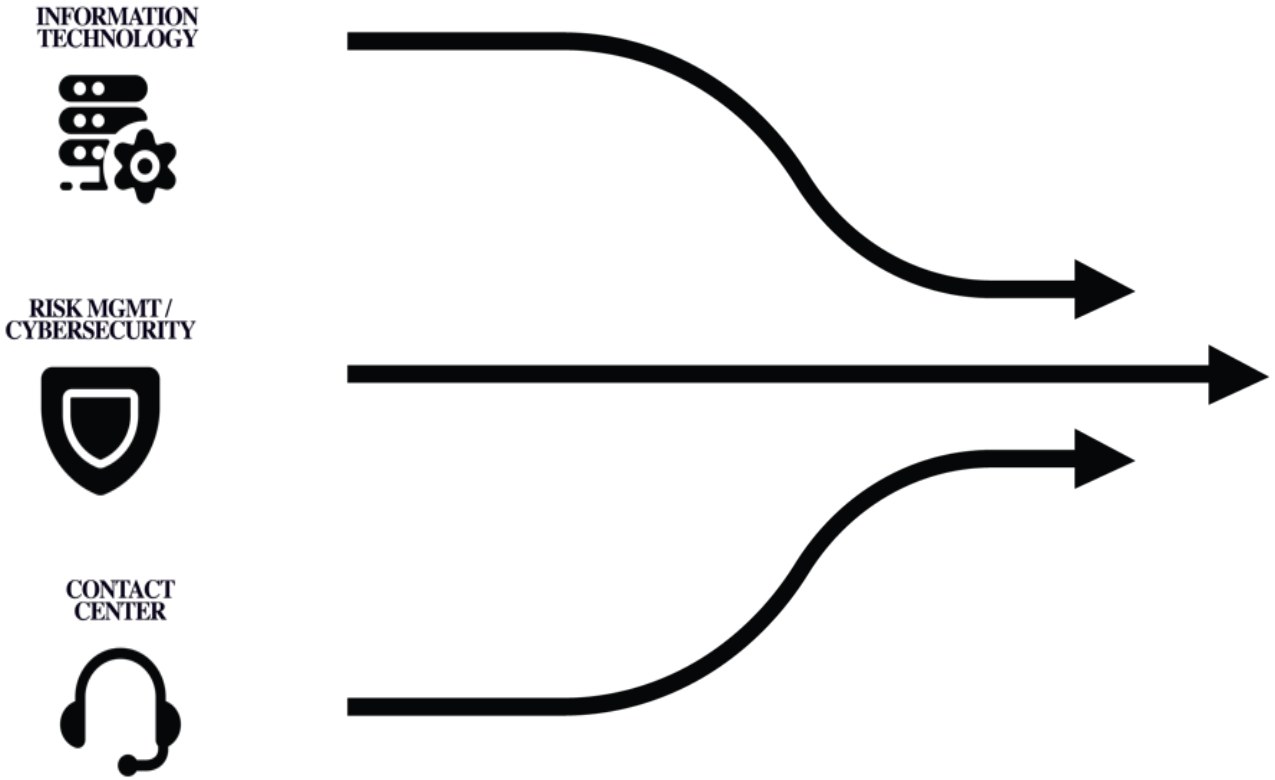
mutare

How to Eliminate Voice-Based Threats & Strengthen Security Posture

HEALTHCARE

mutare

Voice Security Best Practices



DIRECT DOWNLOAD

You will receive an email after this Webinar with a link to direct download the PDF

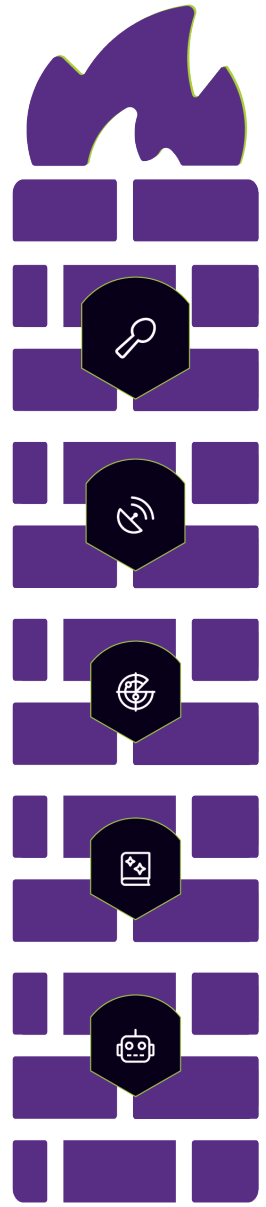
mutare

Our Approach

5-Layers of Protection

- Most Awarded and Powerful Tool on the Market
- 5-Layers of Protection
- Stop Threats at the Network Edge
- Immediately Remove Nefarious & Nuisance Calls
- “Do No Harm” Mandate
- Open Architecture for Simple Integration
- Exceptional ROI

webex by cisco · talkdesk · NICE · Five9 · GENESYS · cisco · AVAYA · Microsoft · IntelePeer



Understand how Voice Threats are impacting your organization

Voice Traffic Analysis

- Client Submits (to Mutare), at minimum, 30 days of CDR data
- Unwanted Traffic is identified through Mutare's Proprietary Dynamic Database of Unwanted Voice Traffic
- Timing: analytics and report production take about 7 business days
- Reports are presented via live or virtual meeting

Proof of Concept (PoC)

- Client implements the Mutare Voice Traffic Filter for 30 days
- Unwanted Traffic can be identified via all 5 protection layers
- Timing: analytics and report production take about 7 business days after the culmination of the PoC
- Reports are presented via live or virtual meeting

MORE INFO ON OUR WEBSITE
https://www.mutare.com/voice-traffic-analysis/

Q & A

Chuck French

Chief Growth Officer

Vicki Sidor

VP, Sales & Channel