Voice Security: Key Impact Zones

Thank you for downloading this Mutare resource. Carahsoft is the distributor for Mutare cybersecurity solutions available via NASA SEWP V, ITES-SW2 and other contract vehicles.

To learn how to take the next step toward acquiring Mutare's solutions, please check out the following resources and information:

For additional resources:
carah.io/mutareresources

For news on Mutare:
carah.io/mutarenews

For additional Mutare solutions:
carah.io/mutaresolutions

For additional cybersecurity solutions:
carah.io/cybersolutions

To set up a meeting:
Mutare@carahsoft.com
(571) 590-7110

To purchase, check out the contract vehicles available for procurement:
carah.io/mutarecontracts

Public Sector

A Flashpoint for Voice-Based Attacks

Public sector organizations are highly visible, data-rich, and often reliant on legacy systems. This makes them a preferred target for adversaries using voice as a weapon of intrusion. Whether the attacker is financially motivated or ideologically driven, the threat is real and rising.

Public Sector: Key Impact Zones

Civic Operations

OVERVIEW

Unprotected or under-protected voice and communication channels hinder government workers' ability to deliver essential public services, respond to community needs, and execute time-sensitive programs.

Nuisance and nefarious calls degrade operational efficiency, delay critical communications, and elevate the risk of service disruption.

IMPACTS OF VOICE-BASED ATTACKS

- Increases response time to constituent / inter-agency calls
- Diverts focus from mission-critical civic responsibilities
- Disrupts continuity of public services
- Reduces system and staff resilience in emergencies
- Delays access to assistance, services, and relief programs

IMPACTS OF A CYBER BREACH

- Operational: Inability to access essential systems (e.g., emergency response, payroll, benefits)
- Financial: Ransomware payments, budget reallocation, compliance fines
- Reputational: Erosion of public trust, media scrutiny, electoral impact

Constituent Experience

OVERVIEW

The voice channel remains a primary point of contact for public sector services. Voice-based attacks degrade access, delay service delivery, and create friction in citizen-government engagement.

When constituents can't reach the right service or fall prey to impersonation scams, trust in government erodes.

IMPACTS OF VOICE-BASED ATTACKS

- Delays resolution of service requests
- Disrupts scheduling of permits, benefits & consultations
- Enables scams targeting vulnerable populations
- Diminishes perception of transparency and competence
- Increases call abandonment and complaint rates

IMPACTS OF A CYBER BREACH

- Constituent data exposure and identity theft
- Increased fraud and public dissatisfaction
- Regulatory investigations and legal exposure
- Breakdown in communications during emergencies

Risk Mgmt / Security

OVERVIEW

Public agencies are increasingly being targeted by cybercriminals and hacktivist groups. Voice-based attack vectors like vishing and social engineering often bypass traditional defenses.

An under-protected voice channel can serve as the initial access point for breaches that compromise sensitive systems and classified data.

IMPACTS OF VOICE-BASED ATTACKS

- Elevates risk of initial access via social engineering
- Reduces efficiency of helpdesk / IT
- Increases risk of exposure for PII, financial data, and internal comms
- Challenges compliance mandates (NIST, FISMA, CJIS)

IMPACTS OF A CYBER BREACH

- Operational: Ransomware and breaches disabling critical infrastructure
- Financial: Cost of recovery, investigations, and regulatory penalties
- Reputational: Diminished public confidence, election consequences

Voice-Based Attacks are Escalating

Nefarious

GEN AI ATTACKS   VISHING   SOCIAL ENGINEERING   SPAM STORMS   SPOOF CALLS

Nuisance

ROBOCALLS   VOICE SPAM

mutare

mutare.com

VOICE SECURITY