EXECUTIVE REPORT

VOICE NETWORK THREAT SURVEY

2022

a proprietary study of the voice channel
and current perspectives of security / risk

Unsecured Voice Traffic, Skyrocketing Adoption of Teams-Centric Enterprise Collaboration Tools Widen Enterprise Cybersecurity Gaps and Increase Risk of Breach

The continued escalation of nefarious and nuisance phone calls to enterprises in the form of robocalls, spoof calls, scam calls, spam calls, spam storms, vishing, smishing and social engineering are the catalyst for an expanding wave of cyber attacks.

Executive Summary

The **Voice Network Threat Survey** reveals serious shortcomings in enterprise security protections against voice network attacks.

Voice Network Traffic is under-appreciated threat vector.

This Report is intended to shine a light on one of the most universal infrastructure systems, the Voice Network, and how the great majority of technology and security professionals are not considering the voice network as a pathway for cybercriminals.

At two recent high-profile technology industry conferences, RSA and Cisco Live, Mutare conducted a survey of event attendees, presenters and vendors to understand the market's awareness of:

- **Voice Network Traffic as a Threat Vector**
- **The specific Tactics used by Cybercriminals**
- **The Impact these Tactics are having on Enterprises**
- **How/If Enterprises are Protecting themselves from this Threat**

In a nutshell, the **Voice Network Threat Survey** clarifies the lack of knowledge, insight and awareness of this real cyber threat. So, in addition to presenting the Survey findings in this Report, we are including some additional content and materials to help educate and explain the problem. Additionally, we have included even more information in the Appendix.

Table of Contents

The Problem

The business telephone, by its very nature, is an open conduit to connect people in an immediate and direct manner.

To technologists and many line of business professionals, the telephone system is known as the Voice Network. It is a core element of every organization's IT infrastructure.

Over the last decade the Voice Network has lost its luster, in favor of a new wave of collaboration tools and applications that began with BYOD and have evolved into integrated chat, web, video meetings, virtual meeting hubs and more. In effect, the telephone has become a utility. We expect it to just work.

But how many of us hesitate to answer our cell phones these days, because it's usually a spoof call, robocall or potential bad actor?

Well, this same situation is happening in every organization. The issue is that the enterprise must answer the phone, there is no question.

At Mutare, we call this the Open Doorway. Cybercriminals are counting on the fact that a human will answer the business phone.

INDUSTRY METRICS

AVG Unwanted Voice Traffic in Enterprise Networks Source - Index of Unwanted Voice Traffic, Mutare	**9%**
Vishing Attack Success Rate Source - How to Attack Yourself Better in 2021, Group IB	**37%**
Fraud Losses Due to Voice Channel Source - 2020 Press Release, FTC	**$3.3B**
US Organizations Faced with Vishing Attacks Source - 2022 State of the Phish, proofpoint	**77%**

Terms & Definitions

What is the Threat Vector?

Voice Network Traffic, also known as inbound and outbound calls and SMS.

Tactics Used by Cybercriminals to Exploit this Threat Vector

- Robocalls
- Spoof Calls
- Scam Calls
- Spam Calls
- Spam Storms
- Vishing (Voice Phishing)
- Smishing (SMS Phishing)
- Direct Nefarious Calls
- Social Engineering

Term for the Calls or Traffic Generated by the above Tactics

Unwanted Voice Traffic

Types of Attacks Resulting from these Tactics

- TDoS Attacks
- Ransomware Attacks
- Data Breach
- Data/IP Theft
- Identity Theft

About the Survey

Key Facts

Format, In Person
Respondents were surveyed live, by a member of the Mutare Team.

When / Where was the Survey Conducted?
The Survey was conducted on the showroom floors of RSA 2022 and Cisco Live 2022.

Data Collection
Survey Responses were collected via a Tablet device. A cloud-based survey application was used to capture all responses.

All Responses were Anonymous
Survey respondents did not submit any personal contact information. This was a true research initiative, and not a marketing tactic.

Data Compilation & Analytics
Standard data compilation and analytics techniques were used to produce result sets and findings.

Survey Questions
Twelve (12) multiple choice questions were included in the Survey.

Average Completion Time
The average time for a respondent to complete the Survey was 2.13.

Survey Questions

1. Which best describes your job function?
2. What is your position level?
3. Which of the following best describes your industry?
4. Approximately how many people does your organization employ?
5. Who is responsible for overseeing voice network security within your organization?
7. What is the biggest source of security risk in your organization?
8. What type of security tools/solutions does your organization use to protect voice network traffic?
9. Does your organization identify vishing, smishing, social engineering and robocalls as major security threats?
10. In the past year has your organization experienced a vishing, smishing or social engineering attack targeting employees?
11. If you answered YES to Q9, What was the source of the vishing, smishing or social engineering attack?
12. Can you estimate the percentage of overall Inbound Unwanted Voice Traffic to your organization?

Respondents by Industry

54% Technology and Innovation 12% Government 9% Education 7% Financial Services 5% Healthcare 3% Legal

Respondents by Job Level

44% Mid-Level Specialists & Managers 27% Senior Executives 13% Entry-Level 9% C-Level

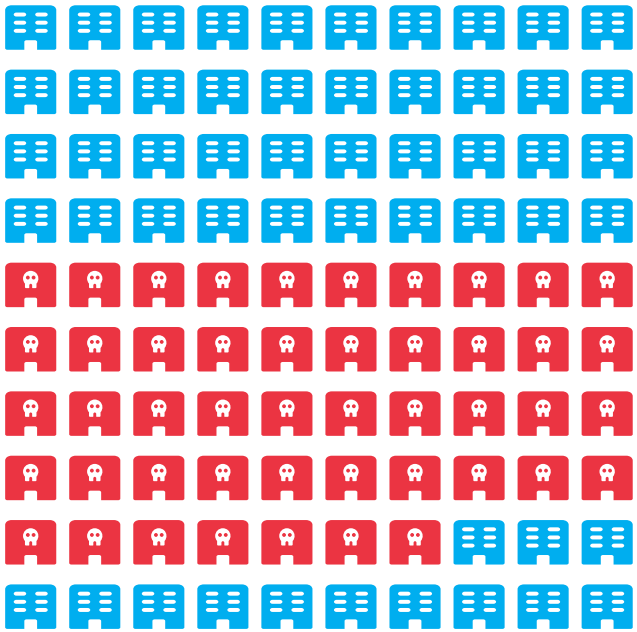
Findings

SURVEY SUMMARY

Serious and costly shortcomings are pervasive in enterprise security protections against voice network attacks leveraging inbound and outbound traffic (calls).

47% Organizations Victimized by Vishing Attack or Social Engineering

Nearly half (47%) of organizations experienced a vishing (voice phishing) or social engineering attack in the past year.

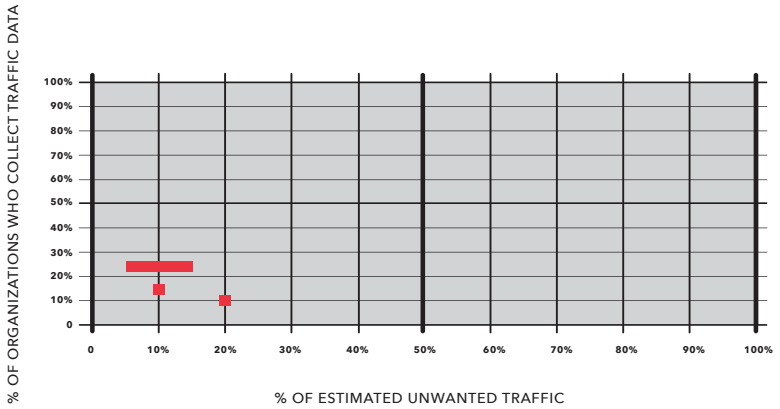


NOTE
See Appendix-A for *Index of Unwanted Voice Traffic*, which shows a breakdown of Unwanted Voice Traffic by Industry.

Findings CONTINUED

38% Organizations Do Not Track Malicious Voice Traffic

Remarkably, more than one-third of respondents to the Voice Network Threat Survey (38%) said their organizations do not collect any data on the amount of inbound, unwanted, and potentially malicious voice traffic hitting their organizations.



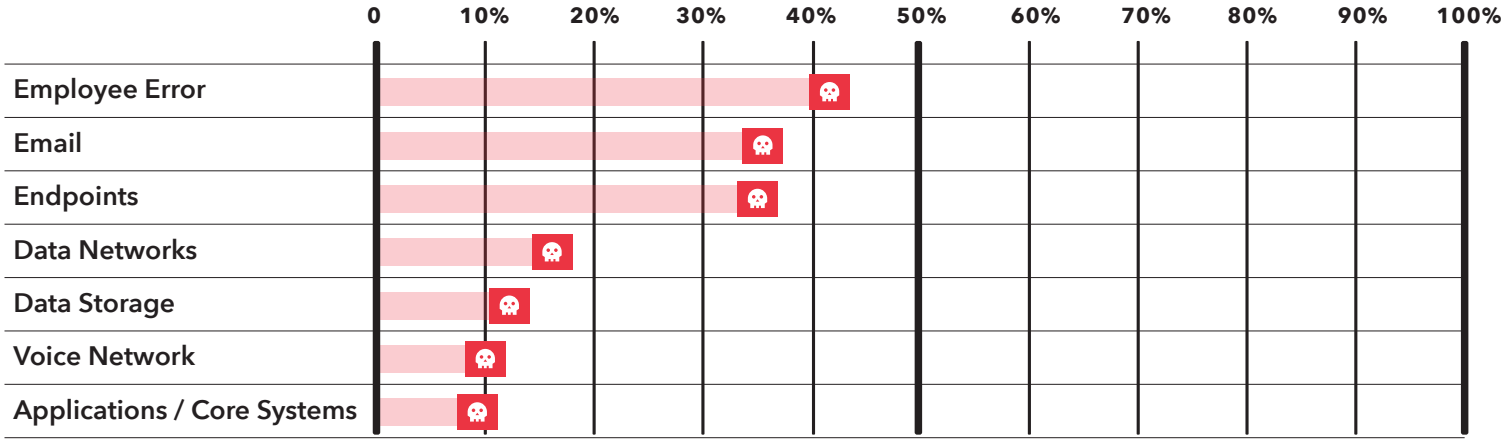
Organization's Estimated % of Unwanted Traffic

Of those that do collect such data, 23% of respondents estimated that 5% to 10% of inbound calls were unwanted, followed by 15% of respondents who estimated that over 10% of inbound calls were unwanted, and 10% of respondents who estimated that over 20% of calls were unwanted.

Findings CONTINUED

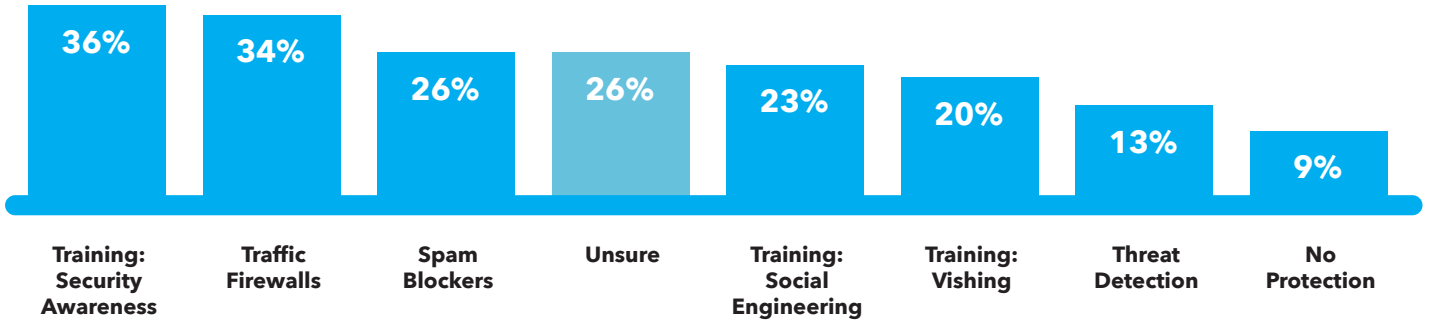
Sources of Security Risk

The biggest source of security risk stems from employee errors, according to 43% of survey respondents. That ranking was followed by the risk from email (36%), endpoints (35%), data networks (17%), data storage (12%), and applications/core systems (9%). Only 10% of respondents cited their voice networks and phone systems as the biggest source of security risk in their organizations, reinforcing a widespread lack of awareness about this problem.



Findings CONTINUED

Solutions Used for Voice Network Protection



More than one-third (36%) of respondents cited security awareness training as the top solution to protect voice networks from Vishing (voice vishing) and Smishing (SMS phishing) attacks. That approach was followed by traffic firewalls (34%), spam blockers (26%), training for vishing attacks (20%), training for social engineering (23%), and threat detection (13%). In addition, more than one-fourth of survey respondents (26%) were unsure about which tools were being used to protect their voice networks, and 9% said their organizations had no solutions in place whatsoever to protect their voice networks.

INDUSTRY METRICS

41% — **41% of Security Awareness Training Programs cover Vishing**
Source: ProofPoint, *State of the Phish*

95% — **95% of Cybersecurity Breaches are Caused by Human Error**
Source: Cybint Solutions, *Cybersecurity Facts and Stats*

90% — **90% of Successful Cyber Attacks Require Human Interaction**
Source: ProofPoint, *Voice of the CISO*

Findings CONTINUED

81% of Respondents Believe that the Voice Channel is a major Threat Vector

More than four-in-five respondents (81%) agreed or strongly agreed that their organizations identified vishing, smishing, social engineering, and robocalls as major security threats.

Given An Attack, Which Component of the Voice Network was Compromised?

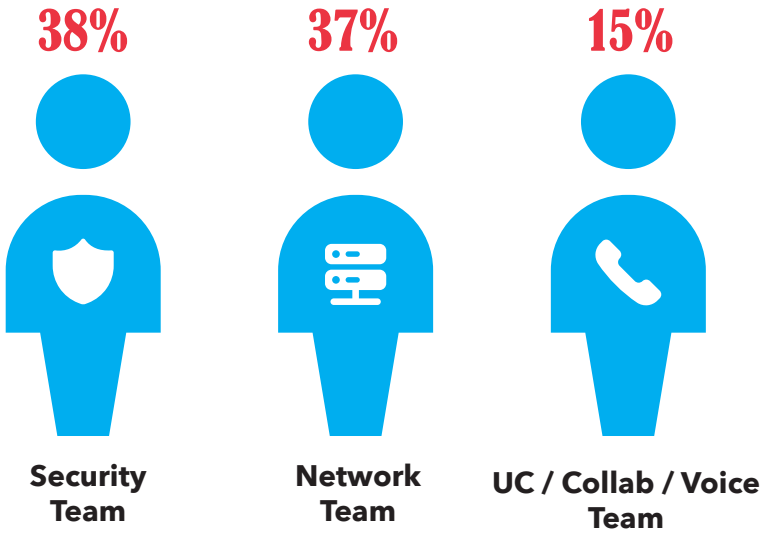
For those organizations that received voice attacks in the past year, nearly one-third (32%) involved SMS/text scams, followed by attacks on collaboration platforms such as Cisco WebEx and Microsoft Teams (16%), and Telephone Calls (14%). 35% of respondents were unsure about what types of attacks had struck their organizations.

- **32%** SMS / Text Scams
- **16%** Collaboration Platforms
- **14%** Telephone Calls
- **35%** Unsure

Findings CONTINUED

What Team is Responsible for Voice Network Security?

The responsibility for overseeing voice security was almost evenly divided between responses for the Security Team with 38%, and the Network Team with 37%. In addition, 15% of respondents cited the Unified Communications/Collaboration/Voice Team as being responsible for their company's voice network security.



Conclusion

Quantitatively, the Survey results show that respondents believe that the Voice Network is an important threat vector that should be managed in order to reduce organizational risk.

Qualitatively, the answers are less straight-forward. Based upon the survey results and our discussions with the live respondents, we see a lack of real connection and clarity when covering the voice channel, voice network and voice network traffic in terms of cybersecurity and cyber protection.

For many of our respondents the Survey Proctor had to explain some of the terminology, including "Vishing" and "Smishing." Given our audience, attendees of RSA 2022 and Cisco Live 2022, this was a surprise, and a clear indication that education is paramount.

Respondents were clear that cybercriminals are actively leveraging a broad range of tactics to attack organizations through the voice network. And, that these attacks are often successful.

What seems unclear is what internal business unit should be responsible for protecting the Voice Network, and what tools or solutions to apply to thwart the bad actors.

Beyond the Survey, all the industry metrics tell us that the problem of unwanted voice network traffic is getting worse.

And, the problem is more than robocalls; the tactics used are trending away from nuisance calls to nefarious calls which are clearly intending to do significant harm.

Most importantly, when the business telephone is involved, **the issue is a human one**. Every organization has to answer the phone. So, your people are going to be faced with protecting the organization against the bad actors.

Training your people is critical, but most Security Awareness Training does not cover phone related scams and attacks. So please, connect with your Training Partner and make sure they include robocalls, spoof calls, scam calls, spam calls, spam storms, vishing, smishing and social engineering.

Synopsis

1. The Voice Network is under attack, and it is getting worse.
2. The Problem includes: robocalls, spoof calls, scam calls, spam calls, spam storms, vishing, smishing and social engineering.
3. Industry Professionals recognize that there is a problem.
4. But, there is no clarity around who is responsible for addressing the Problem, or what technical solutions will combat the Problem.
5. So, many organizations turn to Employee Training to solve the Problem. But, the Training is incomplete and not super effective.

There is a technical solution that removes unwanted voice traffic at the network edge.

see Appendix-B

APPENDIX

- INDEX OF UNWANTED TRAFFIC
- A FIREWALL FOR YOUR VOICE TRAFFIC

APPENDIX - A

Index of Unwanted Voice Traffic

A breakdown of Unwanted Voice Traffic by Industry.

8.70%	All Industries

15.88%	Higher Education	8.32%	Utilities & Energy
7.44%	Healthcare	13.90%	Legal Services
8.84%	Manufacturing	2.94%	Federal & State Government
12.99%	Technology & Innovation	6.80%	Financial Services
3.37%	Retail	6.49%	Other

SOURCE MUTARE, INC.

APPENDIX - B

A Firewall for Voice Traffic

Remove robocalls, spoof calls, scam calls, spam calls, spam storms, vishing, smishing and social engineering calls at the network edge.

Learn more on Mutare.com

https://www.mutare.com/voice-traffic-filter/

SOLUTION NAME

Mutare Voice Traffic Filter

SHORT DESCRIPTION

Enterprise-class software built to provide multiple layers of protection against unwanted traffic. We create a barrier at the network edge, ensuring that malicious and nefarious traffic does not gain access to your network.

CORE VALUE PROPOSITION

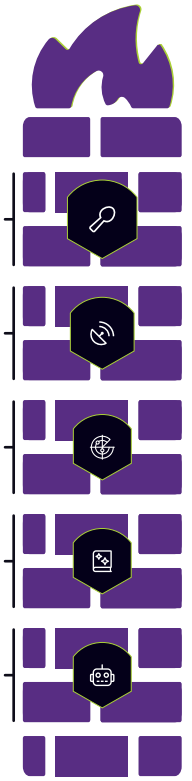
Remove unwanted voice traffic (calls) at the network edge.

HIGHLIGHTS

- Most Powerful Tool on the Market
- 5 Layers of Protection
- Stop Threats at the Network Edge
- Immediately Remove Nefarious & Nuisance Calls (Robocalls, Spoof, Vishing, Spam..)
- "Do No Harm" Mandate
- Open Architecture for Simple Integration (Avaya, Cisco, Microsoft, Mitel and a wide range of UCaas, CCaas, CPaas ecosystems)
- Exceptional ROI

5 Layers of Protection

It's Like a Firewall for your Voice Traffic



1 **STIR/SHAKEN**
Analyzes STIR/SHAKEN attestation scores in call data for evidence of suspected call spoofing.

2 **Proprietary Dynamic DB**
Integrates data from worldwide resources to identify known spam, scam, spoofing and robocalls.

3 **Threat Radar**
Applies a set of analytic processes to detect atypical call patterns consistent with nefarious activity.

4 **Custom Rules**
Creates organization-specific custom rules directing filtering actions for matching calls.

5 **Voice CAPTCHA**
Extra layer of vetting that challenges callers to enter random digits before call is complete.

ASSESSMENT

How is your organization being impacted by Unwanted Traffic?

CUSTOMIZED WITH YOUR DATA

The Voice Traffic Assessment provides you with visibility into the traffic traversing your enterprise voice network. Each Assessment is created and customized based upon your organization's data.

VISIBILITY INTO YOUR VOICE TRAFFIC

Your custom report will uncover and expose the types of traffic traversing your voice network. You will have clear numbers and metrics to understand the scope, scale and impact of unwanted traffic in your environment.

VOICE TRAFFIC ASSESSMENT

(a 21-page customized report)

About

Three Decades of Expertise

For three decades, we've been empowering organizations to re-imagine a better way to connect with each other. Today, through our transformative digital voice and text messaging solutions, we make communications with colleagues, customers and prospects simple, secure and effective. And that means more time and less stress for your employees, a more positive experience for your customers, and improved bottom line results for your organization.

Get to know Mutare

Our forward-looking leadership team is made up of dedicated, focused and experienced people who care about transforming business communications and improving the lives of others. Working together with our employees, their knowledge and experience come together to make a difference for all our stakeholders – customers, partners, businesses and communities. We are change makers.

Headquarters
Mutare, Inc.
2325 Hicks Road
Rolling Meadows, Illinois 60008

Support
855.782.3890
help@mutare.com

Sales
847.496.9000
sales@mutare.com

mutare.com

EXECUTIVE REPORT

VOICE NETWORK THREAT SURVEY

2022

mutare
RESEARCH