Guarding Against
Call Center Fraud and Attacks

A Corporate White Paper
by SecureLogix Corporation

Overview

All corporations secure the Internet connection to their internal data networks with IP firewalls and related technologies. However, most corporations have yet to recognize the serious vulnerabilities they are exposed to by their connections to the untrusted public-switched telephone network (PSTN) or carrier SIP network. Since they do not recognize the threat, they have taken no steps to lock down these voice network connections. But the reality is this: Although attacks against an enterprise's Internet connection receive the most public attention, attacks against an enterprise through the voice network are actually very common and can be very expensive. And external attacks are not the only serious vulnerabilities plaguing your voice network. Many risks originate inside your organization.

Examples of voice network vulnerabilities include these internal and external threats:

- Unauthorized modem use, which bypasses the data firewall and exposes the corporate data network to the unsecured voice network and risks data theft and virus infiltration.
- Long-distance and international service abuse, in which employees misuse voice resources for personal use.
- Long-distance and international service theft, in which on-premises non-employees (such as the cleaning crew) steal voice service to place long distance or international calls.
- Unauthorized access of restricted modems, such as the PBX maintenance port.
- Harassing and threatening calls, including bomb threats.
- Toll fraud, in which an outside attacker hacks into the voice network and steals long-distance service.
- Social engineering fraud attacks, in which callers attempt to perpetrate and exploit identify theft to unlawfully access and steal from your customers' accounts.

For example, many corporations, especially financial and insurance organizations, are falling prey to social engineering fraud attacks conducted over call center phone lines. These attacks mimic Internet- and email-based "phishing" schemes, in which criminals attempt to acquire personal information such as usernames, passwords, and credit card account information by pretending to be trusted entities. However, the attacks are perpetrated over typically unsecured voice network connections. These phone-based phishing attacks are sometimes referred to as "vishing" with the "v" standing for "voice."

The unsecured voice network places financial corporations and their customers at increasing risk for information/identity theft and financial damages. A telecom engineering VP at a large credit union

recently noted that these enterprises have invested large amounts of money and resources to deploy solutions on their IP networks to protect against internet and email-based fraud, network intrusion, and phishing attacks, so perpetrators are increasingly targeting the unprotected voice network. When the voice network is unmonitored and unprotected, tracking and identifying perpetrators and preventing their success is an unlikely proposition.

The only solution lies in applying security concepts used for the IP network to the voice network, specifically, the deployment of in-line security devices on call center voice trunks to support multiple security and monitoring applications, such as a voice firewall, intrusion detection system, automated suspicious call rerouting policy, and call recording. This approach provides the voice network with the same security paradigm and protections that have been present on IP networks for years. Additionally, these security devices support analysis and reporting applications that provide for forensic analysis, trending, and usage tracking.

Understanding the Threat

Two recent call center attacks illustrate threats financial industry call centers face. One target was a leading insurance carrier that also provides banking and investment products. The other was a large credit union.

Each organization was the target of phone-based phishing attacks in which the perpetrators attempted to initiate fraudulent transfers of funds from accounts they did not own. The identity thieves had obtained basic information about a bank account. Armed with this information, they made repeated calls to the bank's call center pretending to be the account holder, each time requesting a small piece of additional information about the account. When they gained enough information to masquerade believably as the account holder, they called back to request a funds transfer to an account to which they had direct access, or to request a wire transfer. If they reached a more experienced agent who refused the transfer, they simply called again to a different agent to request the transfer. Many of these fraudulent requests were approved. Hundreds of thousands of dollars were at risk in these attacks.

Business Processes That Can Mitigate Risk

Without a voice network monitoring and security system, catching the perpetrators of these attacks is unlikely. However, certain business practices can help limit your risk. For example:

- Implement an incident reporting and tracking system with a central repository and responsible person. Ensure that all employees know the procedure for reporting suspicious calls, and that alerts about suspicious activity are sent to everyone in a similar role so they are aware they may be targeted.

- Train all new personnel on your security policies and how to recognize social engineering attempts. Conduct regular retraining of existing personnel. This avoids complacency and keeps security foremost in employees' minds. While you do not want to foster a culture of paranoia, you do want to instill a healthy sense of caution.
- Implement an ongoing corporate communications campaign highlighting security, such as a monthly newsletter highlighting real-world exploits and how they might have been prevented.
- If available, run reports on CDR data to analyze call data for suspicious activity, such as frequent calls from a certain number or exchange.

These measures can help, but for true security, implement a voice network security and monitoring system with real-time firewall, intrusion prevention, and call recording policy enforcement capabilities. The patented SecureLogix® ETM® System is the market leading, first-of-kind voice network security solution that provides an arsenal of tools to detect and avert contact center vishing attacks, in addition to many other types of voice network vulnerabilities.

How the ETM® System Defends Call Centers against Fraud

The ETM System provides an arsenal of robust features for voice network security, monitoring, management, optimization, call masking and redirection, and call recording. These capabilities work together to protect against call center fraud and many other threats. This security arsenal includes the following integrated applications:

Voice Firewall—In a manner similar to the way data firewalls monitor access attempts and activity on the data network, the Voice Firewall monitors and protects the voice network. It tracks, alerts, and blocks individual calls when the call characteristics match criteria you specify in a policy. It can identify and react to the type of call, the called and calling numbers (or even portions of the number, such as the exchange), call time, call length, and other call aspects. It stores call data for all monitored inbound and outbound calls (plus additional data for calls that triggered a firewall rule) in a database where they are available for reporting and analysis with the Usage Manager application.

Voice Intrusion Prevention System (IPS)—In a manner similar to the way a data IPS alerts and protects against possible intrusion attempts on the data network, the Voice IPS guards against potential intrusion attempts and attacks on the voice network. It tracks, alerts, and blocks calls based on calling patterns over time. You specify call characteristics and accompanying thresholds—such as acceptable count of calls from a specific phone number, set of phone numbers, or exchange, in a given time period—in a policy and decide whether to terminate calls or alert personnel when these thresholds are exceeded. A Real-Time Monitor provides an ongoing view of accumulated values. This data is also stored in the ETM Database for Usage Manager analysis and trending.

Call Recorder—The Call Recorder records individual calls automatically when the call characteristics match criteria you specify in a policy. These recordings can be listened to for threatening or suspicious language, such as social engineering fraud attempts and bomb threats. You can use the Usage Manager to correlate the time stamp on the call recording with the call data extracted and stored by the Voice Firewall to obtain a clearer picture of the caller and identify the calling patterns employed. You can then use this information to write Voice Firewall and IPS rules that apply to this caller and to the calling patterns that suggest an attack. Suspicious call recordings can also be saved to use for forensic analysis, legal proceedings against identified perpetrators, and training of staff on recognizing the hallmarks of social engineering attacks.

Usage Manager Reporting and Analysis—The Usage Manager's powerful reporting and analysis tools mine and distill the data in the ETM Database, which contains all call details about every call carried on monitored lines, additional details for calls that triggered Voice Firewall Policy Rules, and details about calling patterns flagged by the Voice IPS.

Call Redirection—Call redirection plans let you automatically route calls from flagged source numbers to a specific extension, such as a more experienced supervisor. This action is transparent to the caller, keeping them from being alerted that you suspect fraud while you gather more information.

Voice Network Security in Action

When the financial call center attacks described earlier occurred, both organizations had the SecureLogix® ETM® System installed and monitoring their call center voice network and were using the ETM Voice Firewall to enforce certain usage rules, such as authorized modem use. Since the Voice Firewall stores data for all calls on monitored phone lines, they were able to use the ETM Usage Manager application's analysis and reporting engine to analyze their call traffic and generate reports identifying calling patterns related to the fraud operation.

In the case of the insurance carrier, a senior call center agent reported a suspect transfer request. A quick analysis by the Usage Manager identified the calling number for that call, and indicated other calls from that number. Other suspicious requests were identified as originating from a specific set of phone numbers. Armed with this information, agents were instructed to forward all calls from those numbers to a supervisor for handling. Features built into the ETM System, such as automated call forwarding to a senior staffer and email alerts, could be used to enhance and automate the protection. The ETM System saved this organization more than $300,000 in this attack.

In the case of the credit union, their staff noticed suspicious calls and used Usage Manager reports to analyze a similar fraud scheme. The reports indicated that the suspect calls all originated from a specific VoIP service exchange. In addition to the Voice Firewall and Usage Manager, this organization also uses

the ETM System's Voice IPS and Call Recorder features. They configured a Call Recorder policy to record the conversations on all inbound calls from the VoIP service's exchange. Since the Usage Manager reports indicated the perpetrator tended to call five or more times in a short period, the staff also defined a Voice IPS policy to send an email to senior call center staff whenever the suspect number called five times in one hour. This alerted them to promptly review the Call Recordings for that period. The ETM System prevented more than $400,000 in fraudulent transfers for this organization, including $40,000 of approved wire transfers that were cancelled after review of the call recordings. An added benefit for this organization is that they use the call recordings of the perpetrators to train their call center staff to recognize the social engineering in the calls, to help them recognize future fraud attempts.

Figure 1 below illustrates a Voice Firewall Policy that stores all call data in the Usage Manager database and automatically sends an email alert to the call center agents anytime someone calls any call center line from an identified suspicious number. It also allows specific authorized modems and prevents all other modem calls.

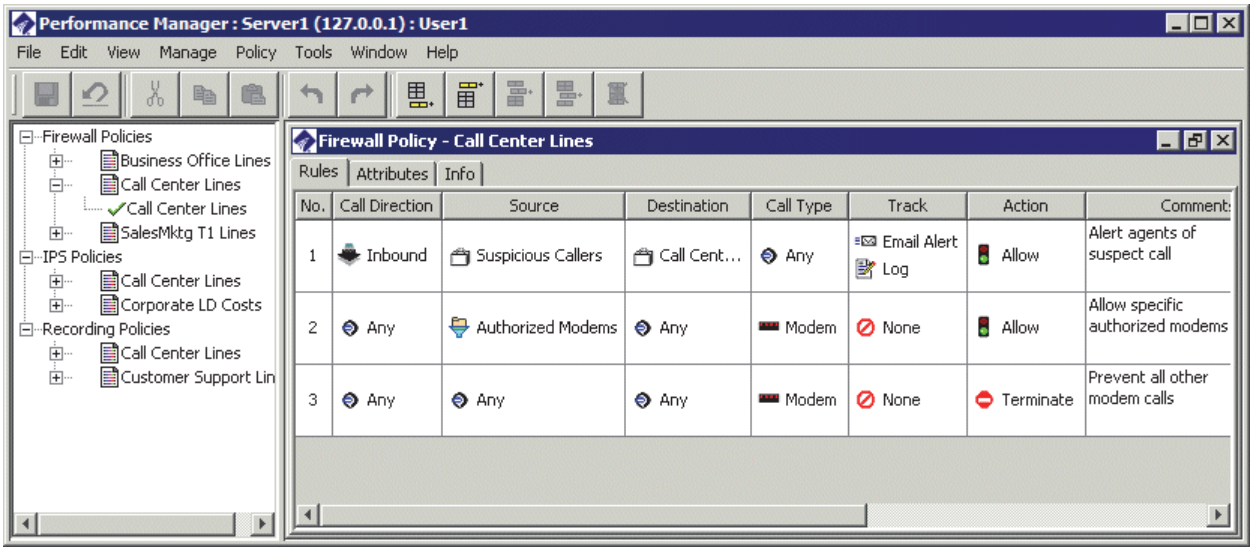

Figure 1: Voice Firewall Policy to store call data, send email alerts for suspicious callers, and prevent unauthorized modem calls

Figure 2 below illustrates a Call Recorder policy that automatically records all inbound calls to the call center. You can also specify that only calls from certain phone numbers—or even certain exchanges—be recorded.

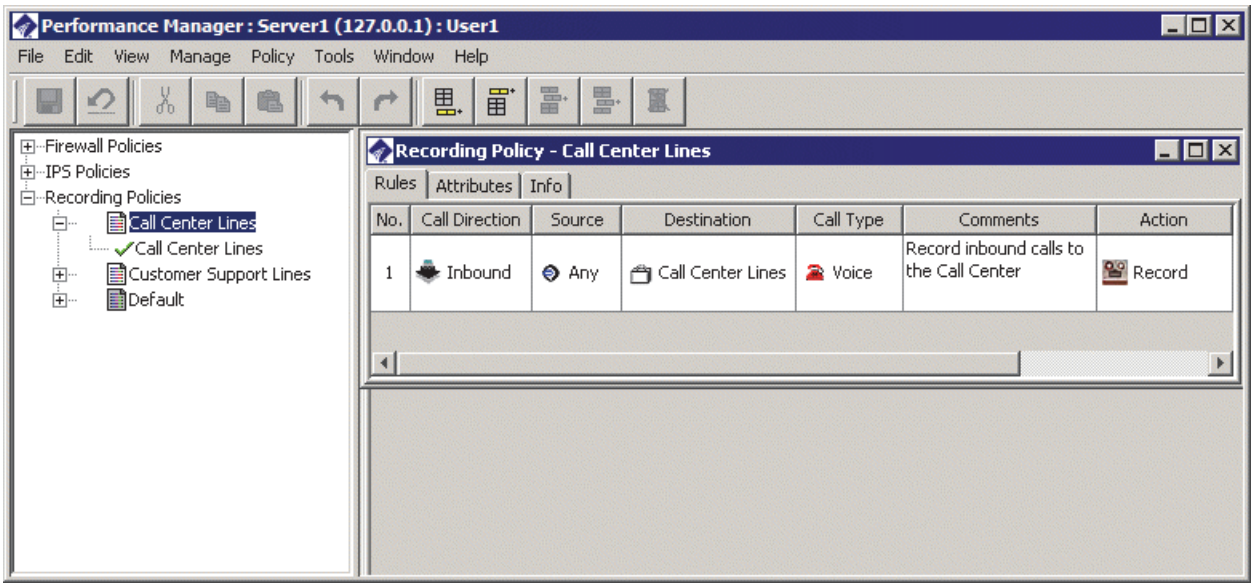

Figure 2: Recording policy that automatically records inbound calls on call center lines.

Figure 3 below illustrates a Voice IPS Policy that sends an email alert when more than five inbound calls come from the same VoIP exchange within an hour. A Real-Time Viewer lets you view ongoing calling patterns without waiting for the rule to fire after the fifth suspect call.

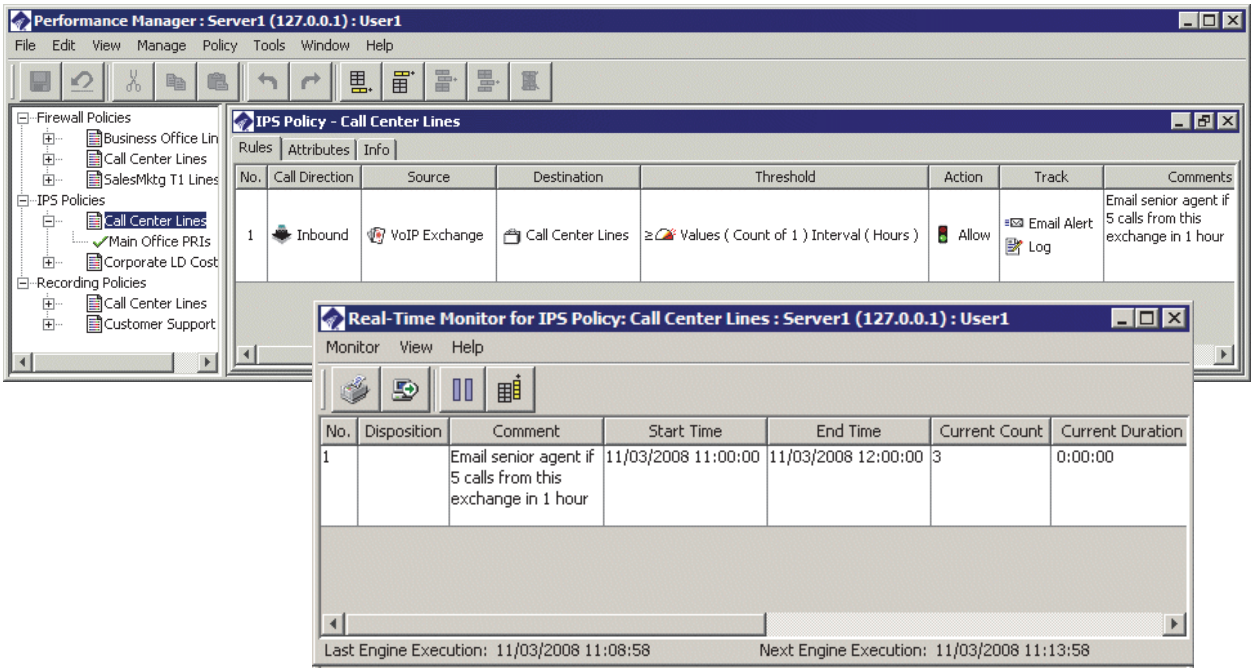

Figure 3: Voice IPS Policy and Real-Time Viewer; policy alerts for multiple calls from the same VoIP exchange, while viewer shows policy enforcement in near real time.

Figure 4 below illustrates a Masking Plan that automatically redirects calls from numbers identified as suspicious to a specific phone number, such as a fraud control agent.

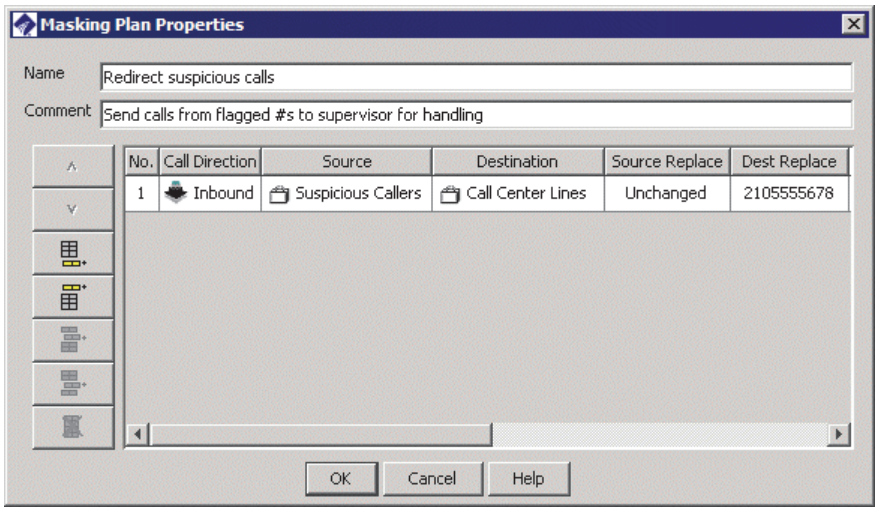

Figure 4: Masking Plan defined to automatically redirect inbound call center calls from specific numbers to a fraud control agent.

Figure 5 below illustrates how you can distill Firewall Policy processing results in a Usage Manager report and then correlate them with call recordings captured by the Call Recorder. The highlighted rows indicate the same suspicious call identified in a Usage Manager report and then retrieved in the web-based Call Recorder interface for audio playback and download for further analysis. While the Call Recorder search in this example is based on call time, you can also search for recordings by other criteria. For example, you might search by source and/or destination phone numbers during a given time period.

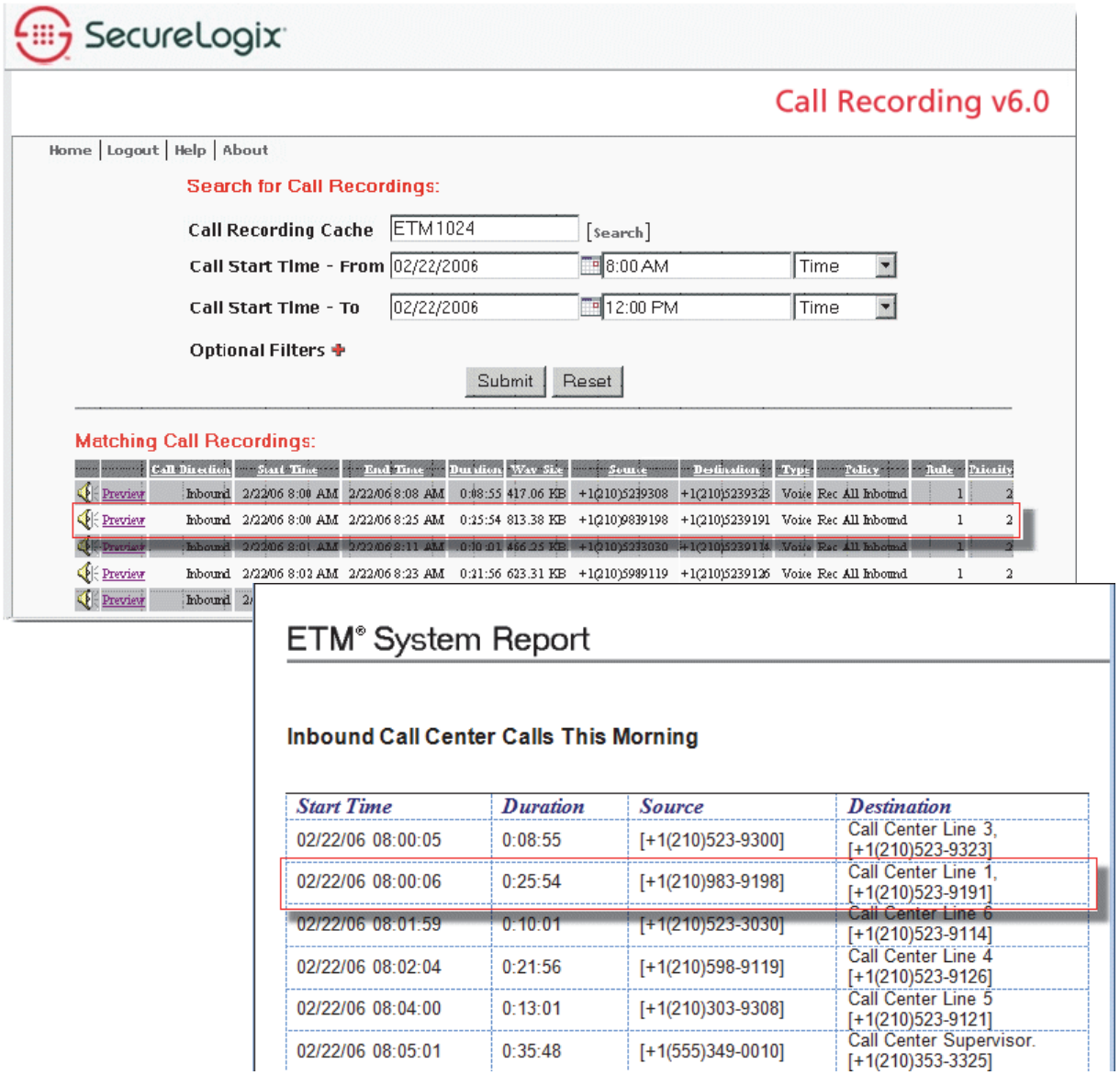

Figure 5: Suspicious call identified in a Usage Manager report; recording of that call accessed in the Call Recorder web-based interfaced for audio playback.

Professional Monitoring by Skilled SecureLogix Analysts

As discussed, the ETM System provides an arsenal of powerful tools you can use to monitor and prevent threats to your voice network. SecureLogix also has a team of expert voice security analysts who can continually monitor your ETM System data to proactively investigate calling patterns and alerts that indicate potential fraud. This service frees you from training and staffing the ETM System in-house.

Return on Investment

A major advantage of this voice network security technology is that, because it monitors the voice traffic into and out of an enterprise, it can produce enterprise-wide data useful for managing trunk utilization, departmental billback, fax utilization, toll fraud, and more. This capability enables the ETM Solution to provide a significant and tangible ROI, in addition to its security benefits.