Unimax

WhitePaper

Strengthen Security and Accountability of Multi-Vendor Voice Systems

HOW UNIFIED VOICE ADMINISTRATION CAN HELP REDUCE EXPOSURE TO CORPORATE SECURITY RISKS.

Strengthen Security and Accountability of Multi-Vendor Voice Systems

Executive Summary

Network security issues are top of mind in every corporate IT organization, and telecom network security is no exception. Threats such as toll fraud, denial of service attacks, impersonation/spoofing, and poor password management cost businesses billions of dollars every year.

Unified voice administration applications, which centralize and streamline the provisioning of telecom assets and the administration of corporate PBX and voice messaging systems, provide organizations with several benefits. These include the reduction of operational expenses, increased system visibility and control, and improved internal customer service. Additionally, voice administration applications help to reduce exposure to corporate security risks. Using real world examples, this white paper will discuss how unified voice administration technology:

- *Tightens the security of voice system environments*
- *Increases audit ability and internal policy compliance*
- *Supports integration to corporate identity management and user provisioning systems*
- *Improves emergency management and business continuity processes*

Introduction

In today's world, security is a key concern for everyone. Corporations, businesses, educational institutions—all must ensure their personnel, facilities, data, and networks are well-protected from a variety of threats. Examples of these threats include software viruses, retaliation from ex-employees, identity theft, and even global terrorism.

Business objectives require companies to effectively counteract these threats while simultaneously reducing costs and working more closely across geographic boundaries and partnerships. How are organizations to balance open-standards and technology advancements with the need for corporate security and increasing regulatory and internal control requirements?

Any time people and systems are connected by networks, new security risks are exposed. Voice systems such as PBXs and voice messaging systems are as much at risk of a security breach as other portions of the IT network.

So what can be done? Limiting the risk exposure by streamlining and centralizing the administration of corporate voice systems can help. Unified voice administration applications reduce security risks involving PBX and voice messaging systems in a number of different ways, as will be discussed in this white paper. At a high level, these methods include:

Strengthen Security and Accountability of Multi-Vendor Voice Systems

- *Tightening the security of voice system environments*
- *Increasing audit ability and internal policy compliance*
- *Supporting integration to corporate identity management and user provisioning systems*
- *Improving emergency management and business continuity processes*

Security of Voice System Environments

Corporate data networks are not the only target of computer hackers. PBX and voice messaging systems are also at risk. In fact, according to a 2003 study by the SANS (SysAdmin, Audit, Network, Security) Institute, an estimated $4 billion per year is lost due to phone fraud. And, on average, each reported toll fraud incident costs around $40,000.

While technical solutions must be in place to secure systems, logistic and administrative procedures are also part of the solution. Securing voice systems becomes even more difficult when considering the multiple systems, multiple vendors, and often multiple teams of administrators that tend to exist within corporations. When each native PBX or messaging administrative system requires a separate ID and password, managing and securing these credentials becomes a challenge.

By locking down access to managed PBX and voice messaging systems, a unified voice administration application increases the security of the corporate voice environment. Voice administrators are allocated IDs and passwords to the administration application but not to the native voice systems themselves. Instead, the administration application stores all PBX and voice messaging system IDs and passwords in an encrypted format. If it becomes necessary to remove or change an administrator's access, it is done within the administration tool.

A unified voice administration application that provides for role-based access also enables administrative activities to be delegated by skill level. The number of master system administrators who have full permissions can consequently be kept low, with the role allocated to a select few. Limited administrator roles can be created and assigned based on authority to manage specific systems or actions. For example, a help desk administrator can be given permission to reset voicemail passwords but not to change any other settings. When creating and automating communication-enabled business processes, role-based administration becomes a fundamental requirement.

Unified voice administration applications provide administrators with increased monitoring and reporting capabilities, which can be used to alert them to potential security concerns within their voice system environment. They can report on the type and frequency of changes, analyze trends

to identify any unusual behavior or patterns, and be alerted to unexpected events, such as when a VIP's password has unexpectedly been changed.

Regulatory and Compliance

For companies publicly traded in the United States, the Sarbanes-Oxley Act had far-reaching consequences. Security and internal control policies were placed in a new spotlight. In fact, Sarbanes-Oxley had such a large impact that in 2005, overall regulatory compliance and Sarbanes-Oxley, specifically, were security managers' top two reasons for protecting data (The InfoPro, 2005). Examples of Sarbanes-Oxley requirements include:

- *Officers will certify the design of internal controls and ensure that relevant information is made known to them*
- *Companies will assess effectiveness of internal controls*
- *Companies will disclose internal control deficiencies to auditors*

In order to show compliance, telecom and IT managers must have the ability to audit systems and processes. Many PBX and voice messaging administration tools, originally developed for legacy TDM environments, are often transaction-focused and don't provide enough visibility or data capture to allow administrators to query historical data, audit administrator actions, or review and troubleshoot related systems. As a result, telecom managers, who are busy focusing on day-to-day management tasks, may not even be aware that data inconsistencies, information gaps, or process inefficiencies exist. These unexplained gaps and inconsistencies become a significant problem during compliance audits and may leave companies vulnerable and at risk for serious consequences and tremendous associated costs.

With unified voice system administration, numerous data fields and reports are available to provide telecom managers with this information. Reporting on information, such as which voice mailboxes do not tie to phone extensions, or which mailboxes do not tie to active employees, can help identify discrepancies which may indicate potential security holes.

Integration with Identity Management Systems

For effective overall corporate security, IT departments must have a coordinated, efficient, and effective process for managing and provisioning IDs, passwords, and computer and network equipment. With an ever-increasing assortment of wireless devices, enterprise application, and user IDs and passwords, correctly provisioning network and telecom assets is no small feat.

Strengthen Security and Accountability of Multi-Vendor Voice Systems

Auditing Voice Administration Policy Compliance: Examples of Types of Reports

For voice messaging systems, a unified voice administration application can list the number and name of mailboxes that have:

- *A given type*
- *Permission to outcall*
- *Permission to access SDLs*
- *Non-conforming naming policies*
- *Membership to a given distribution list*

For PBX systems, available reports include the number and list of phones that have:

- *A given set type*
- *An association with a live extension*
- *An authorization code*
- *Long distance or international dialing permissions*

Additionally, for PBX and voicemail system integrations, available reports include the number and list of:

- *Mailboxes without a corresponding extension, or vice versa*
- *Mailboxes/extensions with mismatched extension display and mailbox names*

For further integrations involving PBX, voice mail systems, and Active Directory, reports include the number and list of:

- *Mailboxes or extensions without a corresponding user*
- *Users with no mailbox number, extension, or phone number*
- *Users with an invalid mailbox or extension*
- *Users with a valid mailbox or extension, but with mismatched user and mailbox or extension display names*

By integrating with Active Directory or other corporate directory services, unified voice administration applications strengthen and complement corporate identity management tools. Instead of two or more separate user provisioning processes—network, desktop, and telecom, for example—one provisioning process is possible. Provisioning of phones, classes of service, and voice mailboxes can be driven based on user profile information in Active Directory, other directory services, or even HR systems.

Strengthen Security and Accountability of Multi-Vendor Voice Systems

Linking unified voice system administration applications with corporate identity management systems also reduces security risk by allowing there to be a single authoritative source of identity information, instead of needing to maintain a second repository for telecom assets.

Streamlining the provisioning process, reducing the number of hands involved, and minimizing the places in which sensitive user information is stored all reduce risk of security breaches, not to mention reducing costs in areas such as identity and role management, auditing, and asset management.

With a more efficient user provisioning process in place, de-provisioning can also be automated and enforced. Within an organization, what is the policy for handling voice mailboxes when an employee leaves? How quickly are they deleted? Are the mailboxes removed from their corresponding distribution lists? Do the mailboxes need to be aged before being reassigned to new employees? If these policies are not clear, or are not reliably enforced, assets such as voice mailboxes can be easily abused by disgruntled ex-employees. A unified voice administration application, however, can ensure these policies are followed.

Emergency Management & Business Continuity

Finally, unified voice system administration applications support emergency management and business continuity contingency plans, should the unthinkable happen.

Automate De-Provisioning and Close the Gaps

A company fired an employee, but neglected to immediately delete his voice mailbox. Months later, the company discovered the former employee was running a small company out of his old voice mailbox number.

At another company, a former employee's mailbox was not deleted, nor was his mailbox removed from an executive distribution list. It took months before the company discovered how sensitive information, which was sent only to select individuals via voicemail, was being leaked on the Internet.

Most companies have de-provisioning or termination policies, but are they always followed? How do they know? If these processes are automated with unified voice administration applications,

Strengthen Security and Accountability of Multi-Vendor Voice Systems

Emergency Management

VoIP and E-911 regulations have placed voice system administration in the forefront of emergency management for large organizations. For 911 calling to work correctly over a VoIP network, each geographical region's Public Safety Answering Point (PSAP) must be able to reconcile the ten-digit number of the caller with their location (Automatic Location Identification data record, or ALI). To ensure this is possible, organizations usually must make sure that any MACs applied to a corporate PBX are also applied to the appropriate ALI database.

Unified voice management tools that can synchronize PBX changes with E-911 databases reduce the manual effort and risk of error involved in maintaining two or more separate databases of information. Reducing the risk of error in this case can increase the response time for emergency medical services.

Business Continuity

Voice communications is a mission-critical activity for most organizations. If employees lose the ability to communicate, operations can be severely degraded or even grind to a halt. During an emergency, unified voice administration can help restore voice communications infrastructures more rapidly.

As an example, when Hurricane Katrina hit in 2005, one U.S. government agency was forced to evacuate 2,150 employees from its New Orleans office. One of the agency's critical priorities was maintaining contact with employees and also helping employees keep in touch with loved ones and friends who were scattered by the storm. Unified voice system administration helped provide uninterrupted voice messaging—a critical point of contact for many employees.

Because unified voice system administration provides a single interface to many different PBX and messaging systems, the administration tool could be used to extract data from one system and import it into another supported system. The software was able to remove important data securely from the New Orleans voicemail system and duplicate it onto another system in Dallas. New Orleans employees could then dial into the Dallas server to leave and retrieve messages.

Without unified voice administration, the agency estimated the manual duplication of the voicemail system would have taken several days, which would have left New Orleans employees without the link to each other and to the outside world that was so critically important in the first few days after Katrina hit.

Strengthen Security and Accountability of Multi-Vendor Voice Systems

The experience of the government agency serves as a clear example of why protecting voice communication infrastructures should be an important part of an organization's disaster recovery planning.

Are we compatible?

Unimax software is compatible with leading PBX, voice messaging and unified communications systems from Avaya®, Cisco®, Legacy Nortel®, Microsoft®, AVST® and others. For more information on specific system compatibility, please email us at TellMeMore@unimax.com.

Conclusion

Among the many pressures facing corporate IT organizations, the need to increase security and accountability repeatedly ranks near the top. Unified voice administration applications centralize and streamline both the tools and processes surrounding the provisioning of telecom assets and the administration of corporate PBX and voice messaging systems. This white paper has shown how by taking control of these processes, unified voice administration technology:

- *Tightens the security of voice system environments by locking down access to PBX and messaging systems and providing role-based administration*
- *Increases audit ability and internal policy compliance by tracking moves, adds, and changes and providing an audit trail for telecom or IT managers*
- *Supports integration to corporate identity management and user provisioning systems to make a single, automated unified provisioning process possible*
- *Improves emergency management and business continuity processes by simplifying PBX database synchronization and restoration processes*

In summary, unified voice system administration technology, while reducing exposure to security risks, also enables automation and standardization—capabilities which provide IT and telecom groups with the added benefits of reduced costs, enhanced system visibility and control, and improved customer service.

For more information on Unimax's Unified Voice Administration products and services, please contact us at (800) 886-0390 or by email at TellMeMore@unimax.com. Visit us online at www.unimax.com.

Unimax Systems Corporation
50 South Sixth Street
Minneapolis, MN 55402
Contact us: TellMeMore@unimax.com

Phone: (800) 886-0390
Fax: (612) 338-5436
www.unimax.com