Securing the Unified Communications–Enabled Enterprise

Integrated communications systems are inherently more secure than traditional standalone phone and messaging systems.

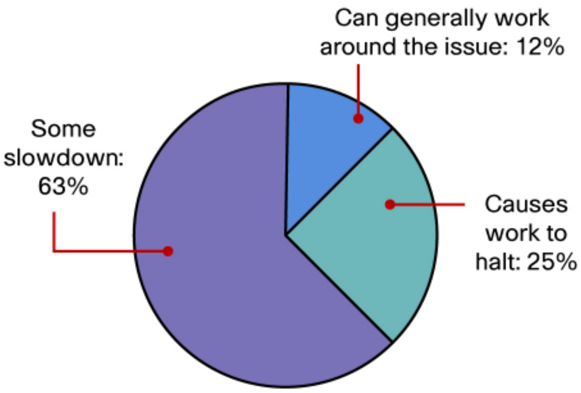
Business Communications Challenges

In today's global economy, traditional time and geographical boundaries are vanishing. Many businesses have adopted a 24-hours-a-day approach to serving customers, who may be located anywhere in the world, in any time zone.

For businesses, government agencies, and academic organizations to thrive in this dynamic market, personnel must remain accessible to colleagues and customers worldwide. Employees—who, like the customers they serve, are geographically distributed and mobile—require the capability to securely obtain information from wherever they are to help their organizations compete successfully.

In fact, research reveals a significant business effect when workgroups experience delays in reaching primary decision makers (Figure 1). Delays are exacerbated when organizations run multiple, standalone systems that do not provide employees with an integrated and secure way to conduct and manage their many forms of communication.

Figure 1. Business Effect of Delays in Reaching Primary Decision Makers



Source: Forrester Research, March 2005 Next-Generation Communications Study

How Cisco Unified Communications Helps

Tying multiple types of communication together into a unified experience supports the increased accessibility needs of global organizations. Cisco® Unified Communications—a set of telephony-focused products and technologies—accomplishes this by merging voice, video, data, and collaboration applications securely across desktops and mobile devices. Cisco Unified Communications consists of a range of Cisco and partner offerings that include integrated IP telephony, messaging, presence (users' location information and availability status), mobility, whiteboarding, and audio and video conferencing. When combined, these collaborative functions boost employee accessibility and, ultimately, customer service.

Accelerated Decision Making

Combining functions so that they work together greatly helps speed internal communication. For example, clicking names in an electronic directory to automatically generate a conference call yields faster information exchanges and decision making than looking up multiple names and numbers in separate directories, dialing them all, and possibly having to leave callback messages. Having both mobile and desktop phones ring when a call comes through helps avoid unproductive telephone tag because employees can answer calls from nearly anywhere. Improved accessibility helps keep business processes flowing.

Improved Call Center and Customer Service

Unifying telephony with customer data also allows call center and other personnel throughout the organization to access up-to-date customer histories. This access to current customer information—combined with chat and instant messaging for quick consultations with colleagues and experts—allows employees ultimately to improve the overall customer experience.

Productivity Gains

Similarly, a single, secured electronic mailbox that collects messages from multiple phones, e-mail systems, and fax machines streamlines the time and effort spent checking and managing multiple messaging systems. These unified mailboxes enhance productivity by making individuals more responsive and by reducing the potential for overlooked messages and delayed replies, which can have costly business consequences.

According to a 2005 study by The Radicati Group, Inc., unified messaging alone can add up to 40 minutes of productive time per worker per day. Sage Research, which conducted a study in 2005 for Cisco involving interviews with more than 200 organizations, reports that workers with access to full-featured unified communications systems gain an average of 55 minutes per day in productivity.

Aside from the basic capital and operational savings that come from convergence, Cisco Unified Communications offers numerous benefits that boost productivity and help companies ultimately compete with better customer service. To fully reap these benefits, however, organizations must make sure that their unified communications networks remain secured. Unified communications brings several new security challenges to enterprise voice networks; however, conversations and messages actually remain more private than in traditional telephony networks.

Security Features and Considerations

Some security concerns and solutions, such as toll fraud, remain the same in the unified communications environment as in traditional telephone networks. Today’s organizations, however, also face increased regulatory requirements for conversation privacy, message confidentiality, and user and device authentication. Therefore, unified communications strategies must address the security aspects of Sarbanes-Oxley, Gramm-Leach-Bliley (GLB), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard, European Basel II, and other mandates affecting global organizations directly within the unified communications architecture.

Integrating security within the underlying infrastructure also thwarts denial-of-service (DoS) attacks, worms, and other malicious activity that is usually aimed at the data network, but, if successful, could have ramifications for the voice network, too.

Here is an overview of how integrated Cisco Unified Communications security provides protection.

Conversation Privacy

As indicated, organizations adding telephone calls and related applications (directories, messaging systems, calendars, etc.) to their corporate data networks must protect the privacy of conversations. Voice conversations are actually more secure in a Cisco Unified Communications network environment than in traditional telephone systems.

The reason for this security is that Cisco Unified Communications systems allow voice conversations to be encrypted. This encryption takes place from phone to phone, so that the conversation remains secured from end to end. As a result, if a would-be eavesdropper were somehow able to tap into an encrypted phone conversation, the discussion would be unintelligible.

Message Confidentiality

Similarly, today's integrated voicemail systems allow enhanced levels of privacy. Businesses can now place conditions on phone extensions that dictate rules about what can and cannot be done. A business, for example, can configure its voicemail system to allow certain messages to be forwarded but to disallow forwarding on messages marked "private." Similarly, the phone system can be configured to allow certain individuals to receive voice messages from third parties through e-mail while restricting other employees from doing so.

Authentication and Verification

Authentication and verification of users, devices, and traffic on a network are essential to any security strategy. An unsecured voice system can sometimes be used as an access point for attacking an organization's data network and disrupting business processes. In such cases, individuals will try to disguise malicious data as voice traffic in hopes that the counterfeit voice traffic will be allowed to pass through traditional data security systems to its intended target.

Cisco Unified Communications systems, however, prevent this from happening. They examine all the traffic on the network, separate voice from data traffic, and then verify that what appears to be voice traffic is, indeed, voice.

Similarly, personal computers controlled by hackers attached to the network masquerading as printers, fax machines, and telephones can serve as launching pads for attacks. Attackers will sometimes use this device-spoofing method to avoid detection and subsequent removal of the unauthorized devices. To prevent such attacks, the Cisco Unified Communications network authenticates all phones, both wired and wireless, and other telephony-related equipment to verify that they are authorized for use on the network. This helps protect the integrity of communications integral to enterprise, workgroup, and individual productivity.

One of the simplest, but most common, threats is an attacker who makes a call and pretends to be someone else to gain access to confidential information. Some businesses have adopted the practice of using Caller ID—the incoming phone number paired with the calling party's name—to identify callers for automated customer service purposes. Unfortunately, attackers have responded to this tactic by sending fake Caller ID information and masquerading as legitimate callers.

Using recently approved worldwide security technology standards, however, unified communications systems now require the calling device to present an additional set of credentials, which are verified by the network. This check helps ensure the authenticity of the device and reduces identity fraud risks.

Foiling Toll Fraud

Toll fraud involves someone dialing into an enterprise's phone system and back out onto a long-distance network to steal phone calls from the enterprise. To protect against this type of attack, the IT or telecom department simply sets up the phone system to disallow transfers to extensions that can make outside phone calls.

Unified Communications integrates capabilities that allow IT or telecom personnel to control the phone numbers that can be used to transfer calls, send message notification, and provide other functions. Implementing the right policies and systems helps prevent access to long-distance phone numbers; in addition, IT or telecom staff can restrict numbers typically associated with toll fraud, such as international numbers.

Preventing Distributed-Denial-of-Service Attacks

Perhaps the biggest threat to unified communications comes from distributed DoS (DDoS) attacks aimed at operating systems and applications in the computer data network. Sound security practices, designed to protect the underlying data network, inherently guard the unified communications system against DDoS attacks and the resulting downtime caused by malicious flooding of the network with bogus messages.

Deployed at strategic locations throughout a network, Cisco Unified Communications security solutions not only detect DDoS attacks but also identify and block malicious traffic in real time without affecting the flow of legitimate, business-critical transactions. As a result, Cisco DDoS products quickly mitigate even the largest attacks, preserve the continuity of your communications traffic, and help ensure that your critical assets remain protected.

Best Practices

Securing unified communications can be successfully achieved by taking advantage of the security capabilities already built into your organization's network infrastructure for data protection. Using best practices for securing the underlying data network infrastructure against viruses, unauthorized access, and eavesdropping is important in protecting voice conversations and related applications.

Securing the unified communications network requires considering voice, data, and video communications as a system and protecting all the system's components, including the following:

- Underlying network and application infrastructure
- Phone switch (also called a call server)
- Individual phones
- Various unified applications

To protect each of these components, enterprises should merge different skill sets throughout the organization, bringing together voice, network operations, security operations, telephone operations, and business decision makers in an interdisciplinary manner.

With more employees becoming geographically dispersed, enterprises should also build in redundant connections from remote locations. This step helps prevent downtime between distributed unified communications equipment and centralized phone switches. IT and telecom staff will be able to logically segment all voice communications-related network traffic from data traffic and help ensure that the voice traffic segment is never sent to data network resources.

Summary

Cisco Unified Communications—a set integrated, telephony-focused applications, devices, and systems that run on the data network—provides a number of benefits:

- Enhanced worker productivity and accessibility, which ultimately increases customer service levels; accessibility is becoming increasingly important in today's global marketplace, which transcends geographic boundaries and time zones
- Higher security levels, which help maintain continuity of critical voice services and address global privacy mandates
- Time savings related to employee communications management
- Capital and operating cost savings associated with network integration and consolidation

Security concerns that arise when adding telephony communications to the network—most notably, DDoS threats—can be addressed by taking advantage of protection already built into the existing data network. In addition, mechanisms in today's systems for encryption and use policies make unified communications conversations and messaging systems more secure than they were in traditional telephony environments. Circumventing toll fraud involves practices similar to those used in the traditional telephony environment.

As your organization adds unified communications applications to the network, you should take a systemic approach to security, addressing all aspects of security in the network infrastructure, including phones, applications, and phone switches. Security also includes building redundant connections from remote locations to ensure continuous unified communications availability.

Securely deploying unified communications requires the cross-functional participation of the expert personnel in your organization, combined with the careful planning, development, and implementation of a comprehensive communications security policy. To assist you in this, Cisco provides a broad range of design, testing, and implementation services to help ensure that your company has a unified communications solution in place with full security.

To learn more about the business value of Cisco Unified Communication, visit http://www.cisco.com/go/secureuc.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA