AberdeenGroup

Safeguarding Conjoined Networks with Telephony Firewalls

An Executive White Paper

September 2000

Aberdeen Group, Inc.
One Boston Place
Boston, Massachusetts 02108 USA
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

Safeguarding Conjoined Networks with Telephony Firewalls

Preface

Data and telecommunications networks are now clearly and irrevocably joined. And the junctions between the two infrastructures are increasing as a result of new capabilities such as Voice Over IP (VOIP). Moreover, suppliers that stand to benefit from the adoption of converged network technologies are encouraging users to accelerate down this track.

Information Systems (IS) executives are sandwiched between suppliers that are strong proponents — and in some cases, users — of conjoined networks, and users already connecting the enterprise's phone and data networks. And many IS executives in early adopter industries are now grappling with the dark side of conjoined networks: the unintended, albeit increased, risk of exposure of the enterprise's sensitive information.

Trail-blazing IS executives are pursuing a variety of strategies for protecting the enterprise from the downside of conjoined networks. These strategies include writing policies that spell out the manner in which the two network infrastructures can be connected, repurposing existing security solutions, and deploying telephony firewalls — a new class of solution designed to safeguard conjoined networks.

Executive Summary

Despite the myriad changes that Information Technology (IT) has seen over the past 10 years, the enterprise still relies on two distinct network infrastructures — data and telecommunications — managed by separate groups and requiring different types of expertise. Both infrastructures are now perceived as critical to the successful operation of the enterprise. And, each infrastructure contains inherent weaknesses that have been and continue to be exploited by insiders and outsiders to the detriment of the enterprise.

IS decision-makers regularly invest in security and integrated security technology to shield their data networks from compromise. In contrast, telecommunications decision-makers have relied on telecommunications hardware suppliers to build in the necessary security capabilities to shield the enterprise. Just as the two infrastructures are largely segregated from an organizational perspective within the enterprise, the approaches to providing security capabilities are dramatically different.

The fundamentally different philosophies for acquiring, deploying, and managing the components used to run the two network infrastructures are now emerging as a problem in many enterprises that have allowed connections between the two networks to flourish. The connections have the effect of undercutting the security approaches inherent in each network, leaving only one constituent of the enterprise satisfied — the hackers.

In this *Executive White Paper*, Aberdeen analyzes the causes of the problems created as a result of joining the data and telecommunications networks and provides insight into how pioneering IS executives are using telephony firewalls to confront and solve the problems inherent in conjoined networks.

IP Networks Are Mainstream

IS buyers have invested huge amounts of capital into enterprise data networks during the past five years, with particularly heavy investment in Internet Protocol (IP) networking technology. The result is a network infrastructure that is far more complex than the mainframe-centric networks that powered the business a generation ago. The current, largely IP-centric networks are far more flexible and connected to far more systems but, arguably, are less reliable than the Systems Network Architecture (SNA)-based networks of yore. But the flexibility has come at a high price: IS buyers are procuring networking components from many different suppliers and integrating the components together to meet the unique needs of each enterprise.

Project-Focused Security Injections

As part of new application development efforts, IS professionals inject new security solutions into the IT infrastructure. Instead of deploying the security solutions as part of an overall security architecture, most IS decision-makers are using the new solutions on a piecemeal basis to solve specific business problems or enable new business initiatives, including the following:

- Issuing user credentials to customers, suppliers, and partners for use with Web applications;
- Extending appropriate access to client-specific information;
- Reducing overhead expenses by shifting from leased lines to Internet-based communications channels; and
- Providing remote users with access to the enterprise's infrastructure without exposing sensitive information to outsiders.

With the rapid transition to Internet-based applications that serve customers, suppliers, and partners, many IS professionals now confront a problem that has been brewing for several years but can no longer be ignored: The boundary — and barrier — between the enterprise and the Internet is blurring. Enterprises that refrained from implementing tight security controls in the past to avoid roadblocks for internal users are now being held back from extending the business to the Internet until the necessary controls are in place.

Despite the claims of many networking suppliers, clothing the enterprise in the necessary security armor is incredibly complex, and the integration challenge is not for the faint of heart. But, because of the risk to the enterprise's brand name

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

and financial well-being, running naked is not an option. IS professionals have taken on the task of deploying a variety of heterogeneous security solutions that enable safe operation in the new digital economy. Those solutions include:

- Digital certificates;
- Firewalls;
- Information access controls;
- Intrusion detection systems;
- Virtual private networks (VPNs); and
- Web authorization servers.

Dial Tone Is More Than Uptime

The criticality of the data network creates a quandary for IS professionals. When users call the enterprise help desk to report the network is down, upgrades, development efforts, and testing all take a back seat. IS staff focus on diagnosing and resolving the cause of the "network" problem and getting the users back online so that business processes — and therefore the business — can be restarted. Even if the cause of the "network" problem turns out to be related to a specific server or application, the IS staff's objective is to get the business back online — at all costs. The data network is now so firmly entrenched in the enterprise's business processes that it simply cannot be shut down, replaced, or dramatically altered.

Incremental Changes in Telecommunications Security

In contrast to the current revolution in the data network security market, the telecommunications security market is mature. Change tends to be incremental and is controlled and driven by suppliers and telecommunications carriers.

In midsize and large enterprises, telecommunications professionals control the internal telecommunications system but have no provisions for ensuring the confidentiality of the traffic outside the enterprise. The telecommunications carriers simply do not offer encrypted VPNs for voice traffic or data traffic running over leased lines.

Moreover, the currently deployed private branch exchanges (PBX) are not designed for filtering inbound or outbound communications in accordance with any enterprisewide security policy. And, because the PBXs are, in essence, closed systems with no provision for integrating policy enforcement capabilities, telecommunications buyers have no obvious alternatives for implementing the needed capabilities.

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

The Telecommunications Dial Tone

The enterprise's telecommunications infrastructure has also absorbed substantial capital infusions during the past five years. But, unlike the data networks, the expenditures for the telecommunications network in the enterprise are periodic, yielding predictable results with very infrequent disruptions in service.

Delivering unparalleled reliability for users, the enterprise's telecommunications infrastructure is rarely a problem. The reality is that the enterprise's telecommunications systems work extraordinarily well and are largely ignored by all but the telecommunications professionals directly responsible for managing the systems on an ongoing basis.

Unlike the enterprise's data network, the telecommunications network is built from components procured from just a few suppliers. The relative homogeneity of the telecommunications infrastructure is a key factor in its numbing reliability. For telecommunications buyers, the homogeneity translates into far fewer integration challenges and readily available expertise from suppliers.

Beyond ad hoc voice and fax services, the telecommunications network is now part of the backbone of the enterprise's customer support infrastructure. Telecommunications decision-makers now factor growth in customer support capability into planning for upgrades in phone service. The telecommunications network is now part of specific business processes.

Moreover, the enterprise's application servers are frequently connected to the telecommunications network at the urging of IT system suppliers. The system suppliers rely on the always available connection to monitor and diagnose problems with the enterprise's servers.

Parallel Networks

For IS executives, the data and telecommunications networks are really two parallel infrastructures. Both are managed by IS professionals, have points of presence throughout the enterprise, and are viewed as critical to the operation of the enterprise. But in midsize and large enterprises, the two infrastructures are treated as distinctly separate entities, with different staff assigned to manage each side of the house on an ongoing basis. And the management staffs responsible for each side of the house treat the network as their own sphere of influence — and brook no interference from their counterparts on the other side of the house.

Conjoined Networks

Despite IS professionals' desire to manage the two network infrastructures as separate and distinct entities, the historical wall between the two networks is eroding, having been breached in most enterprises (Figure 1). The erosion has transpired during the past five years with significant assistance from PC and server suppliers and tacit acceptance by IS and telecommunications buyers.

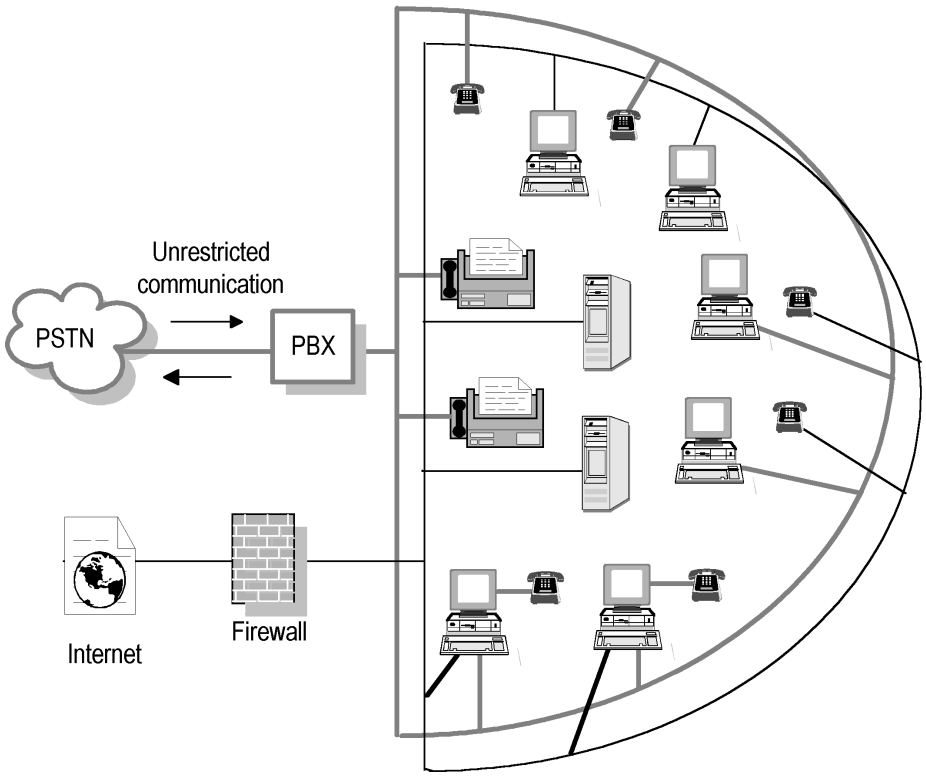
Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

The innocent, well-intended culprit is the ubiquitous modem. Now standard equipment on most desktop PCs, modems are also pre-integrated into the notebooks the enterprise purchases for middle and senior management as well as remote employees. And server suppliers now integrate modems into all but the most inexpensive servers to facilitate suppliers' maintenance and remote diagnostic objectives.

Contradictory Approaches to Security

Charged with providing access to the enterprise's data networks and the applications, information, and servers connected to the network, IS staff view the data network as a critical asset that is available and accessible only to authorized users. The currently deployed authentication solutions, information access controls, network firewalls, and monitoring systems are all deployed to protect the network and network-connected assets from tampering and inappropriate use.

Figure 1: Connected Data and Telecommunications Networks



Source: Aberdeen Group, September 2000

One Boston Place
Boston, Massachusetts 02108
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

Conversely, the telecommunications staff views the network as a highway to which the enterprise and outsiders must have unrestricted access. Although the PBX must be protected from unauthorized access and configuration changes, telecommunications staffs do not attempt to establish or enforce policies with the PBX on appropriate network usage. Unfettered access to the telecommunications network from outside the enterprise is a requirement for customers, suppliers, and partners to communicate with the enterprise.

With the data and telecommunications networks already joined, the currently implemented security measures are effectively diluted. Now the telecommunications network provides unfettered, high-speed access to the enterprise's data network, bypassing the network-edge security solutions intended to keep unauthorized users out of the enterprise network.

Highway to an IS Nightmare

Beyond the concerns that IS executives have about threats posed by unauthorized users at the enterprise's data network and misuse of the telecommunications infrastructure, the conjoined networks present a whole new class of problems that are dramatically more difficult to resolve.

Modem-Enabled Mischief

Although the included modems on PCs and servers provide a degree of redundancy for Internet access and outbound fax, IS staff all too often find that the modems and associated software are configured to permit a wide array of unintended behavior — by employees and outsiders. Once the modems — and therefore the attached PCs and servers — are attached to the enterprise's telecommunications network, the PCs and servers become relay points for any outsider who successfully dials the modem number and correctly interprets and responds to the answering modem's signal.

The possibilities for an efficient hacker are seemingly endless and include the following:

- Reading and altering data on the local PC or server hard disk;
- Accessing sensitive applications and information on other systems residing on the network; and
- Using the enterprise as a launch point for inappropriate activities, including attacking other networks and spamming, while masquerading as a legitimate employee of the enterprise.

The impact on the enterprise ranges from mere nuisance level to exposure of sensitive information and intellectual property to sabotage of the enterprise's reputation. In the worst case — a public disclosure of a successful attack on the enterprise — IS executives may face situations in which valued customers and business

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

partners constrain critical business relationships over concerns about the enterprise's ability to protect its own infrastructure.

Exacerbating Factors

Modems are clearly a weakness in the enterprise's security infrastructure, but they are certainly not the only risk factor that IS professionals must confront. Instead, modems are simply one of a series of weaknesses. Other weaknesses include the enterprise's reliance on Windows 95 and 98 on the desktop and employees' habit of leaving PCs on and connected to the network throughout the work week.

Microsoft's desktop operating systems have been designed to deliver easy access to the plethora of network-connected applications, information, and servers that are critical to running the enterprise's business. And Microsoft has largely achieved this goal, with the unintended side effect of enhancing ease-of-access for everyone — not just the authorized users of the PCs.

Human nature also complicates the picture for IS professionals. Despite the admonitions of IS management — and often with the backing of line-of-business executives — users are oriented toward convenience. And for users, convenience often means leaving PCs powered up and connected to the network continuously. Too many users see a requirement to log off PCs from the network when stepping away from the desk as onerous and simply ignore such policies.

The combination of ubiquitous modems and always-connected PCs turns the enterprise's phone network into an easily accessed pipeline for unauthorized users into the heart of the enterprise's data network.

Users Rely on Modems

The enterprise's employees are frequently active users of PC-modem-enabled applications and services that assist in business processes, including the following:

- Dial-up Internet service provider (ISP) access that enables unfettered access to information and services relating to users' jobs and personal affairs;
- Dial-up access to "bulletin boards" that host software patches and updates for use by the enterprise's engineering and IS staff;
- In-bound and out-bound fax services to provide convenience for individual users; and
- Auto-dialing applications provided with contact information management solutions and fax applications to deliver convenience to users.

The dial-up access to ISPs and bulletin boards creates yet another entry point for viruses, trojans, and hostile applets into the organization, bypassing all the gateways on which IS has deployed anti-virus software and leaving users' desktop anti-

virus software as the only line of defense for the enterprise. The dial-up access and fax software enable users to bypass existing software filters deployed to prevent the transmission of confidential information beyond the enterprise's electronic borders.

Voice Over IP on the Horizon

IS decision-makers are now considering VOIP to augment the current phone network capacity and capability. VOIP offers huge savings in provisioning and operating costs and the ability to deploy a rich set of applications without the limitations imposed by a single supplier. And the technology can utilize excess capacity on the enterprise's data network. But, to date, few IS buyers have taken the plunge.

Telecommunications decision-makers now trialing VOIP are finding that packet prioritization is critical to ensure that the enterprise's data networking requirements do not smother the capacity required to deliver satisfactory levels of service for voice applications. And decision-makers must pay much closer attention to the details associated with the underlying, heterogeneous foundation of the IP network. To be successful, the telecommunications managers must forge new relationships with data network professionals in the enterprise and develop new skills, all of which entails incremental personal risk.

Despite the challenges and risks associated with implementing VOIP services, IS executives will move ahead with the new capabilities, albeit gradually. In the process, the data and telecommunications networks will be joined irrevocably.

Living with Conjoined Networks

IS executives are pursuing a variety of strategies to protect the enterprise from the downside of conjoined networks:

- Establishing written policies that define the circumstances under which users may install and use modems on desktop PCs;
- Mandating the removal of modems from desktop PCs, often with assistance from consultants and systems integrators;
- Deploying security solutions that erect barriers between the data and telecommunications networks; and
- Acquiring new security solutions that enable IS to establish and enforce policies on the connections between and use of both network infrastructures.

Aberdeen's field research reveals that the mixed bag of approaches is actually a progression for some IS executives, with the initial attempt usually based on written policies. But, in many midsize and large enterprises, the written policies are well nigh impossible to enforce. What actually happens, say these executives, is that the enterprise procures PCs without modems, and users then purchase and

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

install after-market modems. And, in some cases, users actually expense the cost of the modems back to the enterprise.

Auditing Desktop PCs

Taking a more activist stance, some IS executives mandate the removal of the offending modems and task IS staff to audit desktop PCs for compliance and, where necessary, remove and confiscate the modems. Alternatively, IS decision-makers turn to a professional services firm to do the dirty work. Decision-makers pursuing this approach note that the process is extremely time-consuming; and, to be effective, the process must be performed continually because some users replace the confiscated devices — again at company expense.

Personal Firewalls

IS executives who have considered or attempted policy-oriented approaches to resolving the conjoined network problem are turning to security solutions instead of relying solely on policies and audits. The security solutions include personal firewalls that are appropriate for use in enterprise environments, along with a smattering of more esoteric solutions that deliver compartmentalization on the desktop.

But personal firewalls must be deployed on each desktop and, to be truly effective, must be managed centrally. The cost of deploying the products on each desktop is daunting to many IS executives. Too many of the current products are simply too complicated for users to deal with on an individual basis.

Compartmentalization products are designed to segregate the PC into separate systems and are appropriate only for environments in which the focus is on risk elimination instead of risk management — usually in the military or intelligence community.

The Telephony Firewall: A New Approach

For IS executives who have tried other approaches to no avail, or rejected them as impractical, a new approach provides relief. A new class of solutions — *telephony firewalls* — provides the policy creation and enforcement capability that enables telecommunications professionals to centrally control how the enterprise's phone network is used and mitigate the risk associated with conjoined networks.

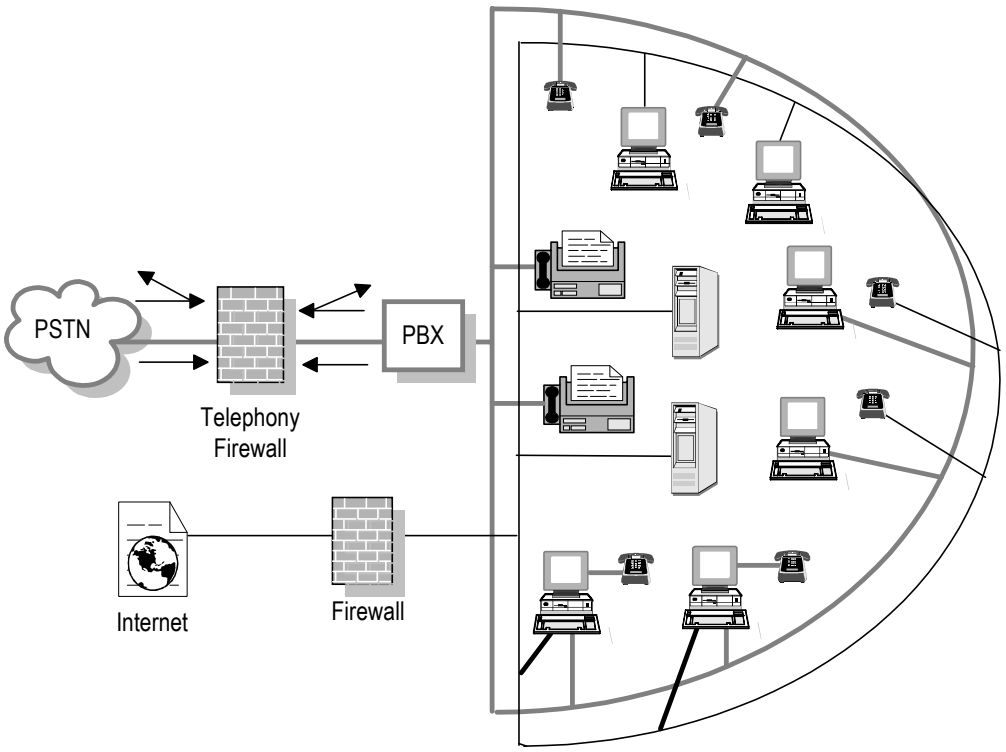
Telephony firewalls are designed to apply established rules for communications to and from the enterprise's phone network and determine whether the communications should be allowed or terminated. The approach will seem strangely familiar to IS professionals with even rudimentary knowledge of firewalls. But this new class of solution is deployed between the enterprise's PBX infrastructure and the public switched telephone network (PSTN) — with no impact on the enterprise's data network infrastructure (Figure 2).

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

IS executives already using telephony firewalls explain that the technology stops outsiders' attempts to enter the data network via the modems in the enterprise's PCs and servers. And the telephony firewall can prevent the enterprise's users from employing the modems in the enterprise's PCs and servers to send faxes and access external services. The solution constrains the potentially offending modems without requiring IS to deploy software or hardware on each PC and server.

Instead, telecommunications professionals deploy the solutions at the telecommunications choke point.

Figure 2: Telephony Firewalls Shield Data and Telecommunications Networks Against Intrusion



Source: Aberdeen Group, September 2000

One Boston Place
Boston, Massachusetts 02108
Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

Characteristics of Telephony Firewalls

Telephony firewalls deliver a unique combination of capabilities and characteristics that provide critical benefits to IS professionals responsible for the data and telecommunications network infrastructures. Telephony firewalls enable IS to set and enforce policies that perform the following tasks:

- Protect the enterprise from external attacks via the telecommunications network;
- Shield the enterprise's sensitive information from unauthorized exposure;
- Reduce costs associated with inappropriate use of the telecommunications network; and
- Curtail behavior that impinges on the enterprise's productivity.

For IS executives who have tried and rejected other approaches to dealing with the risks inherent in conjoined networks, the telephony firewall is a tangible solution to a problem that threatens to undermine the enterprise (Table 1). And it is a solution that the enterprise's employees cannot circumvent to regain the convenience of modem-enabled services.

Complementary Capabilities for Telecommunications Buyers

Telecommunications professionals already using telephony firewalls emphasize the need for an accurate picture of exactly what is attached to the telecommunications network. Without an accurate picture, they can do no more than offer an educated guess regarding the kinds of policies that need to be established. Worse, the decision-makers responsible for the enterprise's telecommunications infrastructure often confess ignorance about what is actually attached to the telecommunications network.

Table 1: Telephony Firewalls Meet Telecommunications Buyers' Requirements

IS Buying Criteria	Telephony Firewall Characteristics
Allow or disallow use of the telecommunications network based on rules established by IS	Yes
Transparent to users	Yes
No integration required with the enterprise's PBX	Yes
Manageable over an IP-based network	Yes
Control telecommunications traffic into and out of the enterprise	Yes

Source: Aberdeen Group, September 2000

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

Although telecommunications professionals usually know what numbers are in service, there simply is not enough time to keep up with the details of which phones, fax machines, or modems are associated with each extension the enterprise uses. And, say the professionals, the picture has to be kept current to ensure that the rules enforced by the telephony firewalls keep the data network segregated from the telecommunications network.

Borrowing Tools from the Hacker Community: War Dialers

Telecommunications professionals can easily turn to the PBX to determine which phone lines are active within the phone network. But, to know how each line is being used, the telecommunications professionals must look elsewhere. Often, the tool of choice for sounding out the type of device attached to the phone line is a high-speed, batch-oriented, automated dialing system, referred to as a *telephone scanner*. But, these tools are also known as "war dialers" and have been around for years. Many were invented by enterprising hackers looking for phone numbers that connect to computers rather than people.

The telephone scanner is a vulnerability assessment tool for phone networks. With a telephone scanner, telecommunications professionals can determine which phone lines are connected to computers, fax machines, and telephone units — far more quickly and easily than they can by walking around the enterprise's offices, labs, and production facilities.

Using the feedback from a telephone scanner, telecommunications staff can establish which devices are actually connected to the enterprise's telecommunications network. Telecommunications staff can then develop the rules that the telephony firewalls must enforce to protect the enterprise from unauthorized disclosure of information, loss of productivity, and misuse of the phone network.

After a telephony firewall has been deployed by the enterprise, the telephone scanners can be used to provide a periodic census of the organization's phone network. The inevitable changes and additions to the phone system can be unleashed or kept in check as appropriate.

Current Usage of Telephony Firewalls

Telecommunications buyers point to the need to keep unauthorized users out of the enterprise network as the preeminent rationale for acquiring and deploying telephony firewalls and telephone scanners. Already intimately familiar with conventional firewalls, these professionals have recognized the risks inherent in parallel, connected network infrastructures.

The early users of telephony firewalls in large enterprises also cite the need to ensure that contractors who provide critical services to the organization do not have the opportunity to take advantage of access to sensitive information, use the read-

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

ily accessible PCs (with modems) to fax information to outsiders, or e-mail the information with the assistance of accounts with local ISPs.

Beyond the concern of contractors having access to sensitive information, IS decision-makers also acknowledge the concern that contractors and employees may be particularly unproductive and use the enterprise's PCs to access the Internet through local ISPs in violation of the enterprise's policy that accords access only to selected employees.

IS executives in enterprises that provide phone support services to customers describe a serious concern about denial-of-service attacks levied at the enterprise via the phone system. Fearing the overloading and eventual shutdown of the enterprise's phone system, IS executives understand the consequences of customers who flee due to poor or non-existent support services.

Less obvious, but just as compelling, IS executives are also comparing the tradeoffs of upgrading the enterprise's PBX to the cost of acquiring telephony firewalls. With most PBX upgrades now performed using a forklift, decision-makers are looking to extend the life of the PBX at least until such time as the asset is fully depreciated. The telephony firewall offers the promise of controlling the increasingly scarce capacity of the PBX by actively enforcing policies that reduce the use of the phone system for extraneous calls.

Finally, executives explain the need to control the volume of outbound calls to keep expenses in line. And, for enterprises that have been frequent victims of telefraud — unauthorized access to the telecommunications network for personal use — the telephony firewall is a sure-fire cost-containment tool.

Increasing Reliance on Telephone Scanners

Aberdeen's field research indicates the vast majority of midsize and large enterprises now have edge-of-network firewall capability deployed as a means of shielding the enterprise from Internet-borne attacks. The research also indicates that vulnerability assessment tools are now being used in a small number of enterprises, lagging firewalls by several years. Although firewalls are difficult to deploy and manage, vulnerability assessment tools are extremely complex and, frankly, daunting to most IS professionals.

But with telephony firewalls and scanners, the reverse appears to be true. Telecommunications buyers are actually acquiring scanners as tools to establish the breadth and depth of the conjoined network problem. And, for those buyers that subsequently conclude that the conjoined network problem is widespread in the enterprise, the telephony firewall becomes the solution to the problem. Deployment of the telephony firewall is actually lagging — not leading — deployment of the telecommunications scanner.

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

As a parallel to the vulnerability assessment services for data networks now offered by managed security service providers, some telecommunications providers are offering telecommunications scanning services to users who require assistance in scoping out the dimensions of the conjoined network problem. For service providers, the scanning solutions provide a basis for a brand new service business.

SecureLogix Offers Telephony Firewalls and Scanners

SecureLogix Corporation is a privately held supplier of telephony firewalls and scanners based in San Antonio, TX. The company's solutions are designed to locate the connections between the data and telecommunications networks within the enterprise and assist IS professionals in keeping the networks safely and efficiently segregated.

The company's signature product, the TeleWall system, is a hardware-based solution that provides firewall-like control for telecommunications networks, and is designed for use within midsize and large enterprise environments. To support a spectrum of user needs, the rack-mountable appliances are available in T1, Integrated Services Digital Network Primary Rate Interface (ISDN-PRI), and 12-line analog versions. The company also provides a management client for use with Windows 2000, NT, 95, and 98 desktops.

SecureLogix also offers TeleSweep Secure system, a telephone scanner for identifying the modems, fax machines, and software solutions connected to the enterprise's telecommunications network. The TeleSweep Secure system is available as both a hardware-based product and a software solution. The hardware version offers ultra-high-capacity dialing for large volume scanning. The software version provides greater flexibility in geographically distributed environments and lower volume scanning.

Category Convergence

Although the technology behind telephony firewalls and scanners is newly productized, the concept is well understood by IT security professionals. They will recognize the simplicity in applying time-tested approaches from the data networking world to the telecommunications networking world.

IS buyers are likely to look to current suppliers for telephony firewalls and scanners, but they will be disappointed in the near term. Traditional security suppliers such as Axent, Check Point, Internet Security Systems, and Network Associates do not provide such capabilities today — nor do telecommunications suppliers such as Lucent and Nortel.

In the cleaved IS organizations of today's midsize and large enterprises, the decision-makers responsible or the day-to-day workings of both network infrastructures will need to cooperate very closely in solving the problem of conjoined networks. For now, buyers must turn to companies like SecureLogix. In time, Axent,

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

Check Point, Internet Security Systems, Lucent, Network Associates, and Nortel will all need to assess this emerging market.

But, over time, the traditional suppliers will cross the line separating the two network infrastructures, presenting decision-makers with offerings that carry strong brand names. The dividing line between firewalls for data and telecommunications networks will blur to obscurity, and vulnerability assessment solutions will include the capability to provide high-capacity telephone scanning.

Aberdeen Conclusions

Conjoined networks are now a reality that can be exploited to the detriment of the enterprise. IS executives are turning to a combination of telecommunications scanners and firewalls as the preferred tools for slaying that dragon.

In addition to protecting the enterprise against the inherent risks presented by conjoined networks, telephony firewalls are valuable tools for controlling and reducing costs and extending the life of the enterprise's expensive and serviceable PBX. Decision-makers point to cost containment and reduction as an additional, compelling reason for acquiring and deploying the new solutions.

But, for telephony firewalls to be deployed effectively, the data networking and telecommunications network professionals must establish new working relationships across a heretofore unbreachable barrier. Although the relationships may be new, there is already a precedent in many enterprises that are deliberately joining the two infrastructures with new applications such as VOIP.

Although users currently have few choices for acquiring telecommunications scanners and firewalls, the options are likely to increase during the next 12 to 18 months as traditional security suppliers and telecommunications equipment suppliers bring new offerings to market. And, just as the professionals within the enterprise must establish new working relationships, suppliers must extend beyond their traditional niches and sell to new players within the enterprise.

The good news for users is that conjoined networks need not expose the enterprise to undue risk. Telephony firewalls that protect the enterprise do not impose changes in behavior on the employees and, for most employees, are transparent and have no negative impact. IS executives who are concerned about the impact of joining the data and telecommunications networks in the enterprise should consider telephony firewalls as a strategy for safely moving forward with converged network technologies.

Telephone: 617 723 7890
One Boston Place
Fax: 617 723 7897
Boston, Massachusetts 02108
www.aberdeen.com

Aberdeen Group, Inc.
One Boston Place
Boston, Massachusetts
02108
USA

Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com

Aberdeen Group is a computer and communications research and consulting organization closely monitoring enterprise-user needs, technological changes and market developments.

Based on a comprehensive analytical framework, Aberdeen provides fresh insights into the future of computing and networking and the implications for users and the industry.

Aberdeen Group performs specific projects for a select group of domestic and international clients requiring strategic and tactical advice and hard answers on how to manage computer and communications technology.