Protect Your Business From the Outside *In*

The New Agenda For Network Security

Preventing Hack Attacks ■ **Disaster Recovery & Business Continuity**

Managing Network Security: The Tactical Battle

new corporate challenge

The explosion of Hacking

(AND WHAT YOU CAN DO ABOUT IT)

THANKS TO RECENT WORM ATTACKS and the grim promise of plenty more in the future, it's clear that we won't be going back to business-as-usual anytime soon.

Here's the truth: when it comes to corporate information security, it's clear that we don't live in Kansas anymore. Instead, the recent onslaught of viruses and worms like last year's Blaster and SoBig attacks have made clear that the corporate fortress is being assailed from all sides, all the time—and the attacks will only get worse. In 1988, Carnegie Mellon University's CERT (Computer Emergency Response Team) Coordination Center reported six security incidents. In 1995, that number climbed to above 2,400. In just the first three quarters of 2003, nearly 115,000 incidents were reported.

Certainly, part of the problem is that there's no perimeter anymore. Who's us? Who's them? Who knows? So many attacks come from inside rather than outside—as many as 75 percent, by some accounts—that building ever-stronger perimeter defenses doesn't help. There are a variety of other reasons that hacking has become such a major threat:

It's easy for the bad guys. Internet-based attacks on networks are easy to launch and hard to trace, making them a low-risk venture.

SAFE PASSAGE FOR E-BUSINESS

Nothing clobbers an e-business initiative more than customer fears about the safety and security of their data. Fortunately, solutions are emerging that can help businesses to boost productivity and customer satisfaction—without compromising data security.

Securing e-mail. Customers at Charles Schwab & Co wanted to access information like 401(k) statements in order to download the information into desktop financial management tools like Quicken—but without the hassles of special document viewers, multiple passwords, or logging on to the Schwab website. The answer: Schwab opted for a solution from PostX Corp. that delivers secure e-mail to any desktop or web-based e-mail client, so Schwab can reach all of its customers.

Portal to stronger sales. After deploying NEC's Enterprise Information Portal StarOffice21 to supplant paper-based and word-of-mouth information sharing, Japan's Parco Space Systems is using its new web-based portal, dubbed PS-NET, to strengthen sales capabilities and information sharing among its 500 employees and 27 locations. Because PS-NET replaces several non-secure, independently developed e-mail systems, it not only reduces overall operating costs by enabling rapid transmission of information between top management and employees, it also has significantly boosted Parco's network security.

PUTTING A PRICE ON NETWORK SECURITY

Nobody can quantify safety—and yet, CIOs must try. Faced with the reality of tight IT budgets and increased spending scrutiny, IT executives must find a way to cost-justify security spending.

"To build coherent security architectures and programs to support them, CIOs and security chiefs need to assess their firms' security risks and develop mitigation strategies," notes Laura Koetzle, senior analyst, computing and security, at Forrester Research. "Once they've done those things, CIOs and security chiefs can ask for budget in terms that the CEOs and CFOs will understand."

"In order to justify the need for increased security, CIOs must be able to outline how time-consuming and costly it is to recover from a security breach," says Sterling Beane, director of technology for West Virginia's Braxton County Public School System. "The aftermath of a security breach or virus attack is far more costly than implementing proper security measures. In this case the old adage is true: an ounce of prevention is worth a pound of cure."

Joe Granneman, PC and network director for Rockford Health Systems and a user of Top Layer Networks' Attack Mitigator intrusion prevention solution, has the following suggestions for how CIOs can make their security case:

• **State the actual risk without over-dramatizing the potential damages of not acting.** "Do not overstate the FUD factor because it can damage your credibility for future projects," says Granneman. "How many times will they believe that the sky is falling?"

• **Explain the technical concepts of potential security problems in clear English.** "Demonstrate the tangible effects of not acting on a potential threat-financial impacts are the most compelling. Do not belabor the technical details," says Granneman.

• **Talk about the things that aren't being funded.** "Talk about potential security risks that are too low or too expensive and don't require mitigation—this can add to your credibility among the members of the management staff when real threats that require fiscal intervention occur," says Granneman. It also demonstrates a realistic attitude towards security spending.

• **Present third-party research that supports your arguments.** "The research should be from sources that will not benefit from your security spending," says Granneman.

"I like to recommend that CIOs look at return-on-negligence (RON)," says Toby Weiss, senior vice president, eTrust Security Management, at Computer Associates. "What's the cost of not doing anything? What is the cost of the status quo? Can we do things better, with tighter security and with lower operational costs?"

These days:
• Source code isn't needed to find vulnerabilities
• Intrusion tools are becoming more sophisticated—they're designed to support large-scale attacks—while being easy to use, even for novices
• Attackers are leveraging broadband connections to launch large-scale attacks

"Many CIOs and security chiefs don't place enough emphasis on security hygiene basics," says Laura Koetzle, senior analyst, computing and security, at Forrester Research. For example, she says that many neglect to enable default-deny on routers where appropriate, standardize on a few security-validated configurations of each operating system, or implement standard processes for receiving, testing, and deploying security patches.

Intense technical complexity. It's understandable. Applications, protocols, and the Internet itself are becoming increasingly complicated and interconnected—and we rely on them more than ever. Meanwhile, in too many enterprises, IT infrastructures have evolved into Rube Goldberg affairs—although they mostly get the job done, they've become too unwieldy to continue to function efficiently and securely. In fact, many are in danger of succumbing to their own complexity.

Staffing issues. Many times, network and system administrators are not sufficiently trained, or given the proper resources to implement proper security procedures.

Blue Cross and Blue Shield of Nebraska Powers its Business with NEC Servers

CASE STUDY WHY DID BLUE CROSS AND BLUE SHIELD of Nebraska decide to integrate NEC's Express5800/1000 series of Intel® Itanium® 2 processor-based servers into its existing data warehousing and business intelligence environment?

An independent licensee of the Blue Cross and Blue Shield Association, Blue Cross and Blue Shield of Nebraska provides health care coverage or benefit administration to more than 640,000 Nebraskans.

According to Steve Grandfield, Blue Cross and Blue Shield of Nebraska's vice president of Information Services, with more than half a million members supported by a complex computing environment, the organization "required a solution that would not only provide us with the ability to support large numbers of users, but offered ease of system management and overall system stability as well."

STREAMLINE OVERALL HARDWARE

The NEC Itanium systems, which will be used initially for enterprise data warehousing and business intelligence capabilities, will also allow Blue Cross and Blue Shield to eventually streamline the amount of overall hardware they have in stock.

"This is a real validation of NEC's innovation and technology to provide solutions that offer breakthrough levels of performance, reliability and scalability," says Larry Sheffield, senior vice president of the Solutions Platform Group for NEC Solutions America.

"We look forward to working with Blue Cross and Blue Shield to integrate our Itanium servers into their existing IT infrastructure and scale their data warehouse to support their ongoing growth."

HIGH PERFORMANCE AND SCALABILITY

"It was also important for us to work with a proven leader such as NEC, whose superior technology as well as its supercomputer and mainframe expertise will pay dividends through high levels of service in a complex computing environment such as ours," adds Grandfield.

THE NEC EXPRESS5800/1000 SERVER SERIES

NEC's Itanium 2 processor-based servers are designed to meet the needs of the most demanding enterprise and technical computing applications. In order to maximize the performance of the Itanium 2 Processor, NEC has developed a high-performance chipset and crossbar switch cultivated through the development of NEC's supercomputer and mainframe technology. With these innovations, the 1000 series not only demonstrates high performance, but also realizes high scalability and high reliability.

To learn more about NEC's Itanium 2 servers visit www.necsam.com/ia64-2 or call 1.866.632.3226.

Empowered by Innovation **NEC**

The Spam Crisis

THE CURRENT WISDOM IS THAT ABOUT 50 PERCENT of all e-mail is spam—and around 30 percent of today's e-mail traffic is infected with at least one worm or virus. That's a lot of e-mail, considering that by 2006, e-mail traffic will exceed 60 billion messages a day.

How can companies fight the problem? Here are a few ideas:

Beyond text filtering. When media company Network World, Inc. realized that spam accounted for almost 90 percent of the 30,000 e-mails it received every day—and then figured out that each piece of spam cost at least 5 cents,

adding up to $250,000 per year—it became clear that they needed to go on the counterattack. Using only a text filter on e-mail, IT staffers spent as much as six hours a day trying to keep up with spammers' ever-changing strategies. But after installing SurfControl's E-mail Filter, Network World reduced IT time spent on e-mail filtering to less than an hour per day while also cutting the false-positive rate (when a legitimate e-mail is mistakenly treated as spam) to just a quarter of 1 percent.

Getting bandwidth back. Since implementing SurfControl's Web Filter, the U.K.'s Royal Cornwall Hospitals

Trust has reclaimed at least 40 percent of its available bandwidth, which had been lost to non-work-related surfing and downloads. Meanwhile, complaints from medical staff about encountering pornography while online have dropped by more than 90 percent.

Invisible encryption. To ensure its compliance with the Health Insurance Portability and Accountability Act (HIPAA), California-based Catholic Healthcare West turned to Tumbleweed Communications' Secure Public Network, which it deployed at the server level so end users would be shielded from message encryption requirements. Also eliminated: the costly and complex administration of certificate management between entities.

Quarantine. Tumbleweed's solutions protect Catholic Healthcare West's internal infrastructure from incoming e-mail laden with viruses, spam, or denial-of-service (DoS) attacks. To dodge destructive virus attacks without the hassles of a virus patch, Catholic Healthcare West quarantines .vbs messages using Tumbleweed Secure Policy Gateway so messages never reach employee desktops and network performance is not affected.

Crashing the Internet

AS OF THIS WRITING, THE INTERNET HAS NOT YET been brought down by a denial-of-service attack, but some experts believe it's only a matter of time. Certainly these attacks, which choke off legitimate network traffic by bombarding certain servers with illicit traffic, have and will continue to force targeted businesses to a standstill. The costs, of

WHAT'S TODAY'S RISK FACTOR?

Internet Security Systems' Internet Risk Impact Summary for the second quarter of 2003 shows that the number of serious security incidents increased nearly 14 percent over the first quarter of 2003. Meanwhile, the number of new vulnerabilities grew by 20 percent, with more than 700 new weaknesses identified.

- **Industries most attacked in 2Q 2003:**
- **Services—24 percent**
- **Financial and insurance services—19 percent**
- **Retail—16 percent**
- **Manufacturing—11 percent**
- **Government (federal, state, local)—8 percent**
- **Food and drug—5 percent**
- **Information technology—4 percent**
- **Healthcare—3 percent**

course, can be enormous: lost sales, employee productivity trashed, negative publicity.

Consider the distributed DoS attacks launched over the 2004 Super Bowl weekend: aimed mostly at online gambling sites, they started on Friday and continued through the weekend, peaking at 200 megabits per second. Many were "cyber shakedowns" launched by extortionists who threatened to keep attacking until protection payments were made. Some sites, however, deflected the attacks using Riverhead Networks' XT Series of appliances, which filter out malicious traffic using active mitigation capabilities that rapidly detect attacks and separate malicious packets from legitimate traffic.

WHEN IT COMES TO NETWORK SECURITY, NEVER ASSUME ...

... That the internal network is safe. "Internal networks can't offer the same level of protection as external networks," says Joe Granneman, PC and network director for Rockford Health Systems. "Guard your LAN ports with physical security or port-based authentication."

... That your greatest security risk is from a hacker. "Studies have shown that potential damage from employees and consultants far exceeds the risk from external hackers," says Granneman.

... That your management team understands the actual risks posed by data security issues and the potential financial loss.

... That your software vendors are versed in data security issues. "They will request access levels from you to make their work convenient, not secure your enterprise," notes Granneman.

... That any one security device is sufficiently capable to deal with threats. According to Granneman, "The best security is multi-vendor and multi-layered with overlapping roles."

... That your staff is designing security into new projects.

Adds Christian Byrnes, vice president and service director at META Group, "A little bit of paranoia goes a long way toward solving security problems."

Automotive Exchange Securely Manages Access for Thousands of Member Companies

CASE STUDY **COVISINT IS A GLOBAL SOLUTIONS** provider founded by the world's largest automobile manufacturers, including DaimlerChrysler, Ford and General Motors, to improve the effectiveness of mission-critical processes such as collaborative product development, procurement, and supply chain management. Through the Covisint exchange, manufacturers and suppliers conduct business efficiently and securely, enhancing members' cost structure, time to market, and the quality of goods and services.

Not surprisingly, says Dave Miller, chief information security officer for Covisint, "an exchange environment poses rigorous security challenges. You want to make the system so convenient that members can't imagine doing business any other way. Yet you need to provide a level of security that will satisfy your users and auditors alike."

COST EFFECTIVE, DRAMATIC SCALABILITY, EASILY ADAPTED

"When Covisint started, we only had 200 companies and 5,000 identities. We needed a secure web access management solution that worked from a cost standpoint yet would allow us to scale dramatically. RSA ClearTrust® software has enabled us to do that. Today we securely manage access for over 135,000 users from 25,000 companies spread across 96 countries, and those numbers are growing daily," says Miller.

RSA ClearTrust software from RSA Security Inc provides Covisint with a single electronic identity and point of connectivity for each user, single sign-on (SSO) across member sites, and easy administration of user access privileges. On the security side, the web access management software erects high barriers to intruders, ensuring that sensitive information is not revealed to competitors, and federating user identity information so it can be securely passed from one member company to another.

"In the old days, an engineer who worked for a supplier might have IDs for 10 different Ford systems," says Miller. "When that engineer moved to another supplier, you were lucky if five of those IDs were removed. That individual could still access sensitive information. Now, when that engineer leaves, the employer can turn off his access to 50, 60 or 70 systems with one operation."

Miller also noted that RSA ClearTrust software is easily adapted. "The auto industry has well-established ways of handling identity management," he says. 'For example, IDs are associated with special numbers and supplier hierarchies. RSA ClearTrust software provides hooks that allow me to write custom items that 'look automotive.' In turn, this makes the Covisint environment more appealing to companies in the industry."

For more information on how RSA ClearTrust software can secure you, visit www.rsasecurity.com

RSA SECURITY®

Protecting their company from such malicious attacks is only one of the strategic investments CIOs need to make in security technology. The first step is developing an overall policy.

"One of the biggest challenges CIOs face while implementing and managing network security is understanding their overall security posture," says Greg Gotta, Symantec Corp.'s vice president of gateway and network security.

Steve Purdham, CEO of web- and e-mail-filtering solutions provider SurfControl, sees five clear steps that CIOs must take to solidify their security strategy:

1 Identify what information and resources are critical to your organization.

2 Identify the risks—what happens if the information is lost or the resources are misused? "These are not small tasks, but clearly defining the problem is critical to the overall success of your strategy," says Purdham.

3 Define a policy that protects the organization.

4 Adopt technology that will allow you enforce this policy across all areas of your network, for both the local and remote workforce. "Many corporate security risks are to

> ## "About 40 percent of enterprise organizations are continuing to underfund security.

the company's information," Purdham says, "which is why a complete security solution must go beyond the firewall." CIOs should add technologies such as web and e-mail filtering—as well as technology to manage instant messaging and peer-to-peer applications—to other physical security solutions such as encryption, intrusion detection and authentication.

5 Train all your employees on how to prevent risks from entering your network.

"There are three major drivers for security: regulations, risk mitigation, and cost reduction," says Toby Weiss, senior vice president, eTrust Security Management, at Computer Associates. "Any effective security strategy must address all three." **sd**

How to Get Control of Spam Without Compromising Performance

CASE STUDY LIKE MOST COMPANIES, CompuCom saw its volume of spam explode exponentially–and its staff grow anxious for relief. But when Chris Odom and Travis Parker, members of CompuCom's network services team, went looking to upgrade their content filtering solution, they had more on their minds than blocking spam.

What they wanted was to improve users' experiences by reducing the volume of spam without compromising performance. What they needed was a solution that would enable them to get control of spam, reduce false positives, and be scalable as well as flexible. But to deliver, the solution had to address a number of issues. Even getting control of spam, it turns out, was not straightforward for the giant IT services and system integrator.

RULES AND FALSE POSITIVES
"Even with the strong anti-spam agents available in products today, none we found was powerful enough to block the amount of spam appearing daily at CompuCom's gateway,' explains IT manager, Parker. "What we needed was the ability to develop customized rules that, when used in conjunction with the anti-spam agent, effectively blocked unwanted content."

Of course, solving the spam problem by creating additional rules often results in the generation of false positives–and most people, maintains director of network services, Odom, have "zero tolerance for false positives." The answer, of course, is to "rewrite the

rule to prevent the block. The problem is how to quickly identify what rule was violated in the first place."

PERFORMANCE AND SCALABILITY CONSIDERATIONS
Performance and scalability were other considerations. Because CompuCom's volume of mail could fluctuate dramatically, Odom and Parker needed a solution that could easily scale to meet demand. And they were committed to maintaining performance, with "delay of the day's internet email unacceptable," adds Odom.

After evaluating five alternatives, including service-based arrangements, CompuCom selected SurfControl Web and E-mail Filters.

Today, CompuCom has a content filtering solution that effectively blocks 79.9% of spam on a volume of 85-90,000 messages daily, helps to reduce false positives via a message administrator function that makes it easy to find and analyze the reasons for blocked messages, is flexible enough to accommodate customized rules and rules changes, includes a centralized database functionality for quick scalability —and meets CompuCom's performance requirements.

"We were impressed with SurfControl's feature set, flexibility and its concise, understandable graphical user interface," adds Odom.

For more information visit www.surfcontrol.com

SurfControl®

new corporate challenge

INVITATION ONLY: Identity Management Strategies

WHEN IT COMES TO IDENTIFYING users and authorizing their access to corporate networks and applications, the limitations of using passwords have become painfully evident. Passwords are easy to guess, easy to hack, and easy to steal using techniques that range from keystroke loggers to phishing. Moreover, they're a management nightmare.

Still, points out Art Coviello, president and CEO at RSA Security, "There are smart, simple alternatives to static passwords that enable organizations to avoid potentially expensive and damaging security breaches that can occur both inside and outside the firewall."

The new alternatives

A NUMBER OF ALTERNATIVE APPROACHES TO IDENTITY and access management enable administrators to centrally manage authentication, authorization, and access across increasingly web-services-enabled enterprise IT environments.

- **Token-based two-factor authentication.** To gain access, users must produce two identifying factors. One is something like a personal identification number (PIN) that only the user knows. The other is something only the user has, such as a token with a unique and frequently changing access code generated by a secure source. This system provides more robust proof of identity than passwords and can be leveraged across multiple applications.
- **Biometric-based two-factor authentication.** Because the second identifying factor is something the user has that's difficult for someone else to steal and misuse (a finger-

print or a retinal scan, for instance), this kind of authentication is regarded as stronger than token-based two-factor authentication.

- **Smart cards.** By consolidating employee badging and security onto a single programmable device, smart cards can lower infrastructure costs (even though card readers must be widely deployed) and make access easier for authorized users.
- **Digital certificates and encryption.** Tough to mimic or intercept, encrypted digital certificates must be retrieved by users from secure servers and presented before access is granted. Proof of identity is considered strong because a trusted third party has vouched for the certificate holder. And since the certificate is encrypted, it's unintelligible to the unauthorized and very resistant to attack.
- **Web access management.** By enabling administrators to centrally manage user access privileges across various networks and domains—including single sign-on across multiple applications—organizations can get rid of multiple security schemes and maintain exhaustive control over access to resources.

"Identity and access management technologies help an organization establish trust in its online environment, ensure the security of its corporate data, and add tangible business value to existing applications," says John Worrall, vice president of worldwide marketing at RSA Security. These new solutions can reduce costs, improve customer service and retention, streamline business processes, and increase employee productivity. Says Worrall: "They are critical components of any security infrastructure."

For example, when U.K.-based consumer credit data supplier Experian signed up new users for web access, its paper-

based system processing took 48 hours—and an average of 2 percent of the user population called in each month for a password reset. Since implementing RSA Security's ClearTrust web access management solution, new users now sign up online, and most password resets are performed without IT help, resulting in lower account administration costs and better client satisfaction and security.

Automated user provisioning

AS MORE AND MORE COMPUTER APPLICATIONS ARE extended to a widening array of employees, partners, and customers, managing application security is becoming impossibly complex.

Automating account provisioning can help. Solutions from such vendors as Courion Corp., Waveset, and Business Layers enable the creation and deletion of accounts and user IDs without system-by-system administrator intervention. The efficiency and return on investment such solutions deliver has prompted major network and systems management vendors such as Computer Associates and IBM/Tivoli to add automated account provisioning to their suites of solutions.

For example, just automating password resets can save significant money. Gartner Inc. has estimated that each one costs $20 and takes about 7.5 minutes while users are authenticated. No less than 30 percent of calls to enterprise customer support centers involved password problems, according to Gartner. Many companies use technology such as Courion's PasswordCourier to solve the problem.

At Atlanta-based SunTrust Banks, each password reset request took 11 minutes and accounted for some 25 percent of helpdesk call volume. Since implementing PasswordCourier, SunTrust password resets are done in a minute or less. **sd**

SunTrust Banks on Courion's Automated Provisioning

SunTrust Banks, Inc. operated as an organization of 28 banks up until 2000 when it organized under a single bank charter. The bank's combined infrastructure included multiple operating systems and custom and legacy applications. The bank was comprised of different business units and approximately 30,000 users (employees and contractors), which required the equivalent of about 60 FTEs for user administration.

As SunTrust set out to upgrade its identity management operations, key business drivers included: immediate enforcement of corporate termination policies; fully auditable account management process; improved provisioning SLA's; easier end user access, and reduced user administration headcount.

BRANCHING OUT INTO ROLE-BASED ACCESS CONTROL

SunTrust deployed Courion's Identity Management Suite™, anchored by AccountCourier® and PasswordCourier® for integrated user provisioning and self-service password management. SunTrust leveraged role-based access control with its on-line and retail banking division.

A self-service portal, now being deployed, will enable managers (whose groups have been defined in roles) to provision employees with very little information, specifically employee name, role, and location. Behind the scenes, Courion's AccountCourier discovers required technical information, and through roles and business rules knows what access to grant.

DRIVING OPERATIONAL EFFICIENCY: SELF-SERVICE IDENTITY MANAGEMENT

Adding automated provisioning and self-service password management resulted in a positive trend in end user adoption, and cost, security and service improvements. PasswordCourier generated immediate cost savings through the reduction of password-reset calls to SunTrust's help desk. AccountCourier provided an added layer for enforcement of termination policies across the enterprise, and broad support of platforms and provisioning functionality.

When fully defined roles and a fully automated auditable account management process are realized, SunTrust's service level agreement (SLA) for on-boarding a new employee will decrease from days to just minutes.

For more information on identity management optimization, visit www.courion.com/cso or e-mail cso@courion.com

Are NETWORKS Out of Control?

IN MANY ORGANIZATIONS, THE "ENTER-PRISE network" is actually an arcane, ad hoc complex of separate, autonomous services that supports diverse applications running at the behest of various enterprise functions and lines of business. Organized, it isn't.

It's all far too convoluted, and managing such a complex infrastructure requires a throng of protocols to master, a multitude of service agreements and maintenance contacts to track, a horde of programs to patch. Total sum of this equation equals some serious cash.

What's more, getting a coherent view of a complex, multi-layered, multi-protocol network is tough. So inefficiencies—traffic bottlenecks, under-utilized bandwidth, duplicate facilities—are inevitable, and vulnerabilities, such as undetected single points of failure, remain unrecognized and unaddressed.

"In many ways," observes Chris Zannetos, president and CEO of Courion Corp., "our industry has not been fully prepared for the operational and organizational issues created by ubiquitous computing and ubiquitous access." This situation will only be further exacerbated by the advent of wire-

PHASING IN BUILT-IN SECURITY

Like many new ways of doing business, building security into applications and networks is best accomplished in phases.

Phase One

PHASE ONE

Train your developers and system architects.

Conduct pre-production application level vulnerability testing of both critical and non-critical apps that includes feedback to developers and regular reassessments.

Thoroughly test your DMZ for vulnerabilities with an eye to root causes and systematic solutions.

Deploy application-level firewalls for moderately- as well as critically-important web-based applications.

Phase Two

PHASE TWO

Conduct a thorough vulnerability assessment of your internal network, focusing on root causes and fixes.

Initiate regular application-level vulnerability scans.

Deploy intrusion detection systems and accompanying monitoring and response processes at key network access points—and until then ensure that log files on critical network devices are habitually reviewed.

Create and adopt a systems development process that ensures security requirements are addressed and met throughout the development lifecycle.

Keep training your developers and system architects.

FIVE STEPS TO NETWORK SEGMENTATION

WHEN YOU UNDERTAKE NETWORK SEGMENTATION, EXPERTS ADVISE THAT YOU FOLLOW THESE STEPS:

1 Talk to others who've done it successfully in environments like yours so you can leverage their experience. Many organizations segment networks into a DMZ, a semi-public segment (mail servers, web servers, basic DNS service), a trusted segment (accessible only by trusted hosts), and a private segment (hosting user workstations and allowing only outgoing traffic flow).

2 Make sure you know your network well before starting any segmentation design work. For instance, what protocols does your business depend on? Although TCP/IP has become dominant, you may find that other network protocols still play an important role.

3 Be aware of how network segmentation may impact your operations model. Example: if your monitoring protocol is SNMP or ICMP, what will segmentation do to your service levels?

4 Understand your network traffic. You need to grasp the details and the larger patterns, so don't rely on a one-day traffic sample.

5 Use a small pilot project to develop a network segmentation strategy and then implement in increments.

less, PDA, Internet cellphone, and other technologies, he says: "As always, the understanding of the operational challenges lags the understanding of the business opportunities created by these technologies."

Building security into the network

THE REALITY IS THAT CIOS NEED TO FIND A WAY TO build security into the bones of the network. For starters, they need to build in lots of availability, scalability, and management automation into both applications and the network infrastructures that support them. Doing this requires a comprehensive, top-down view of the ways applications, systems, network infrastructures, and security safeguards interconnect.

Meanwhile, threats to the enterprise network are intensifying. Once upon a time, security threats were mostly single-mode, making them easy to eradicate with a single product. But no longer. Today, we face blended threats of such complexity that the solutions to address them must combine the capabilities of several security products.

One answer is network segmentation. Ever since routing protocols have become commonplace in business networks, the importance of network segmentation as a security strategy has grown. The issue: routable protocols (of which TCP/IP is the supreme example) are designed to link anywhere with everywhere else, so they're being used by more and more organizations and individuals—as well as by criminals who exploit them to launch the likes of MyDoom, SoBig, and Slammer.

Because network segmentation physically separates a network into distinct parts, it provides a means to manage the flow of routable traffic and protect data and applications. A network segment has its own firewall (implementing rules appropriate to its needs), can have it's own hub or switch, is typically assigned a contiguous range of IP addresses, and may include many machines or just one.

Data moving between network segments must pass through segment firewalls, and high-risk public servers are generally located in a heavily monitored network "demilitarized zone," or DMZ, where attacks can more easily be isolated and controlled.

For example, the SQL Slammer/Sapphire Worm, which struck in January 2003, caused an estimated $1 billion in damage. However, one Fortune 500 company that operates more than 100 process control networks worldwide escaped unscathed. How? By using risk-based network segmentation, 75 CyberGuard VPN/firewall appliances, and e-DMZ Security's Co-Managed Firewall Service, which provides 24/7 event management and production support. Within two minutes of the Slammer attack, e-DMZ was able to query the company's entire environment and determine that none of the firewalls was allowing access through the affected port.

No wonder network segmentation is widely used in security-intensive special-purpose networks, such as those supporting funds transfer, process control transactions, and research and development.

WHAT'S A BLENDED THREAT?
- Uses multiple methods to attack and/or propagate
- Causes harm, sometimes in multiple ways
- Automated, so can be triggered without user action
- Exploits vulnerabilities

Braxton County Public Schools Finds Affordable Network Security

CASE STUDY TO GET THE NETWORK SECURITY functionality he needed, Sterling Beane, director of technology for the West Virginia-based Braxton County Public School system, found himself facing the prospect of implementing a piece-meal solution built by cobbling together products from various vendors

What's more, as the only person experienced enough to install and manage the system he would, most likely, be doing all the work himself across the school's nine locations–with budgets so tight, help was not likely. It was an impossible situation, recalls Beane, with a "learning curve that was just too big and an implementation curve way too daunting."

What he needed was a way to integrate all the functions he was looking for into a single, easy to use solution that he could manage from his office. And in 2003, he found exactly what he needed with Symantec's Gateway Security 5400 Series solution.

FUNCTIONS INTEGRATED AND MANAGEMENT CENTRALIZED

"This product is everything I was hoping to find," reports Beane. "It has all the functionality I wanted including firewall protection, automatic spam blocking and intrusion detection. And because it's all inte-grated, I can centralize the management. And I was simply amazed at the through put," he adds. "I expected a slow down, but my Internet connection is not one bit slower than it was before."

Today, Beane can easily look at any of the boxes on his network across the nine campuses, checking to see if anyone is attempting to hack in and, if they are, what methods they're using. Moreover, he can proactively use the analysis to pinpoint areas where Braxton can make changes to enhance security. Most importantly: he can do it all himself.

And as the sole person responsible for keeping Braxton's network secure, Beane also appreciates how Symantec Security Response keeps him updated.

"I don't have to worry about updating the antivirus definitions, intrusion detection signatures, or content filtering lists," explains Beane. "I just set the time I want updates to happen and they do; the box updates itself and Symantec will notify me if there's a new threat.

"This is an affordable solution—even with the limited resources of a public school system," he adds. For more information about Symantec's solutions, visit www.symantec.com

The Intelligent Network

IN THE END, THE GOAL IS TO BUILD A NETWORK THAT can apply a level of intelligence to security issues.

"Businesses need to take a more holistic approach to security instead of the protect-the-perimeter approach employed by many companies," says Hossein Eslambolchi, chief information officer and chief technology officer at AT&T.

Thus, AT&T is evolving its network and the managed services it supports by it toward what it calls "application awareness." The plan calls for a single, global photonic infrastructure that automates and simplifies every application by providing built-in network intelligence that anticipates user needs, self diagnoses and self-heals to keep the network running smoothly. The result:

- **Dynamic deployment** of applications to maximize server utilization, boost user experience, and cut capital outlays.
- **Automatic deployment,** distribution, scaling, and disaster recovery of web services, web applications, SIP applications, and dynamic content.
- **Self-provisioning** of virtual private networks (VPNs) so enterprises and their applications can be linked with customers, suppliers, and employees.
- **Reliability,** security, and business continuity built into every layer.

"Today's hybrid security threats require tighter integration of multiple technologies," says Eslambolchi, "and a carefully planned defense-in-depth strategy incorporating some aspect of all security elements." **sd**

the tactical battle

COME TOGETHER: Integrating Enterprise Security Management

"LOOK AT THE AMOUNT OF DATA that security professionals are faced with," says Toby Weiss, Computer Associates' senior vice president, eTrust Security Management. Firewall systems, intrusion detection systems, access control systems, hosts, etc.—each produces too many events for administrators to deal with. Bottom line, says Weiss: "Integration between security solutions and between security and network/systems management is essential."

For example, integration is the motivation behind Symantec's Enterprise Security Architecture, an integration platform comprising a Java agent, a web application server, relational datastore, an LDAP directory, and a web browser-based console. The platform does the following:

- Manages several Symantec products, including Enterprise Firewall, Intruder Alert, and AntiVirus;
- Collects data from third-party applications and forwards it to other third-party management systems;
- Offers a role-based administrative domain model that allows delegated administration along physical or organizational lines, as well as event management or product policy configuration lines;
- Provides a unified policy configuration management system that can be used across all Symantec Enterprise Security products.

This kind of integration enables greater flexibility in managing the security lifecycle—threat awareness, policy definition, implementation, and monitoring—by bringing these elements together into a common management paradigm.

Or into a single appliance. Symantec's Gateway Security 5400 Series, for instance, integrates firewall, virtual private network (VPN), antivirus, intrusion detection and prevention, content filtering, anti-spam, and high availability and load balancing components into an appliance that protects networks at the gateway to the Internet or subnets of larger wide-area and local-area networks (WANs and LANs).

Top Layer Networks' Attack Mitigator intrusion prevention solution stops hybrid attacks such as HTTP worms, DoS / DDoS attacks, protocol and traffic anomalies, IP spoofing, SYN flood attacks—in real time—allowing network administrators full control in selecting how the device will respond to detected attacks. Precise but flexible actions against blocking malicious and suspicious traffic include monitoring, alerting, limiting, and blocking.

"By eliminating the need to deploy and manage multiple security products from different vendors," says Greg Gotta, vice president, gateway and network security, at Symantec, "integrated security appliances deliver comprehensive protection while reducing total cost of ownership."

Indeed, integrating and centralizing security management functions can save vast amounts of IT staff time and resources—not only because tasks like virus updates can be handled automatically without relying on end users, but also because once updates and patches are applied, the chances of being successfully attacked drop considerably.

For example, Computer Associates' eTrust InoculateIT has allowed the Plano, Texas, Independent School District to manage virus updates on 23,000 workstations from a single point of management—each workstation is updated every time a user logs in. Denial of service attacks are prevented because eTrust Inoculate IT also locks down desktop agents so users cannot access settings.

After deploying eTrust Antivirus, Audit, and Intrusion Detection, Colorado Springs School District 11 decreased the amount of time needed to detect and repair virus damage from 3,500 to 52 hours per year. Server uptime, formerly "more down than up," is now almost 99 percent.

"More security doesn't make you more secure—better management does," notes CA's Weiss. "The company that knows where their IT assets are, what the vulnerabilities are, and has the correlating technology to find out what is really happening in the overwhelming sea of security data they are receiving will fare much better than a company that doesn't have this kind of management in place."

Should you outsource network security?

MORE FLEXIBLE AND DYNAMIC OUTSOURCING arrangements— made possible mostly by advances in network management systems and remote technologies—offer new ways to get help with network security. Indeed, Forrester Research reports that more than 70 percent of Global 3500 companies use managed services, notably for disaster recovery and hosting.

Outsourcing network security can offer the following advantages:

• **Flexibility and control.** "Co-managing still provides the best combination between outsourcing and in-sourcing," says Kris Zupan, CISSP, chief executive officer/chief technology officer at e-DMZ Security. "As network volatility increases, these benefits will become more important."

Zupan notes that the increased complexity and speed of

attacks are requiring constant monitoring and skilled professionals to react and respond.

• **Global View.** Managed security services providers also tend to have a more global view of the infosec landscape. Conversely, the pervasive nature of attacks and sometimes dramatic steps required to deal with them (like shutting down a mail gateway or isolating an infected network) will put more emphasis on the internal control of the security tools at a company's disposal.

• **Application infrastructure hosting.** The enterprise retains control over an application, outsourcing all infrastructure management. Servers, software, data, network connections, firewalls, and so on may actually be remotely located and operated by the service provider, whose environment may be

An Elegant Firewall for a Dangerous Mission

Controlling access to mission-critical systems is the goal of every organization. But for some, including one for the world's largest chemical companies, the stakes can be very high indeed. According to the company's Chief Security Officer (CSO), a firewall breach can compromise finely tuned process systems, impacting business and potentially "threatening employee safety and the environment."

After September 11th 2001, one of the company's top priorities was to ensure that its 200 plus high-and medium-risk manufacturing process sites were guarded by the most compelling firewall solution available. Lacking the security expertise in-house and believing this is one of the situations that warrant seeking expertise from the outside, the CSO went looking for help. What he found was a unique solution from Managed Security Service Provider E-DMZ Security. According to this CSO, what makes e-DMZ's approach so compelling is the rich environment e-DMZ Security wraps around firewalls, "the way they architected the entire security solution."

THE DIFFERENCE IS THE ENVIRONMENT

Foremost, all communications and control are encrypted, ensuring security is tight; and there are

authorization and audit trails, so every change, no matter how small, is logged, approved and documented.

And unlike other offerings, e-DMZ had already done the work needed for centralizing firewall management and control of the chemical giant's 200+ distributed sites – all of which have firewalls unique to their process requirements. The sites also have process engineers with little or no firewall expertise. Fortunately, e-DMZ's solution was designed to be distributed under just such conditions, making implementations cost-effective and timely.

Another compelling feature is the ability to co-manage. For safety and security reasons, it's essential that process engineers be able to make changes without being inhibited by the firewall.

"We had to ensure the engineers who own those processes would have access whenever they needed it and e-DMZ provided the flexibility without compromising the audit trail," reports the CSO.

"e-DMZ came in with the technology we needed already wrapped around the firewall; it is, quite simply, elegant."

For more information on how e-DMZ Security can protect you, visit www.e-dmzsecurity.com

Hands-on control over your network, day and night

CASE STUDY "A LOT OF SERVICE PROVIDERS ARE moving to web-based customer care to enhance their customer care and to increase efficiencies," says Sandra Palumbo, a senior analyst with the Yankee Group. "AT&T is the furthest along at this point. Anecdotal evidence indicates that customers are very pleased with it."

COST-EFFECTIVE MANAGEMENT

Why are customers so pleased? One reason is the way the AT&T BusinessDirectSM Portfolio of eServicing capabilities enables a business to cost-effectively manage its AT&T relationship around the clock:

· **The AT&T BusinessDirect Web Portal**

AT&T BusinessDirect is a secure, award-winning web portal that enables you to perform a variety of network and routine supplier-management tasks. BusinessDirect Map, provides point-and-click management of an organization's AT&T inventory and view of network elements.

"AT&T is committed to setting a new benchmark for the industry, process automation and simplification, empowering customers with network visibility and control, and collaborative networking capabilities," says Bob Sloan, AT&T eSales & Service Vice President. "By putting advanced networking tools into the hands of our customers, AT&T is giving businesses real-time, end-to-end visibility into their cross-application environments to help them cut costs, gain market share and link with their customers more effectively.

· **AT&T eBonding**

For customers that submit very high volumes of electronic transactions, such as service orders or trouble reports, AT&T eBonding is the answer. AT&T eBonding enables a customer's internal systems to interact directly with AT&T's internal systems so they don't have to re-key data into a web browser.

"No other competitor has a capability similar to AT&T's eBonding B2B platform, which can help significantly increase a customer's efficiency and productivity," Sloan explains. "AT&T's core network support systems are linked directly with large business customers' purchasing, accounting and maintenance systems —giving companies unprecedented access to network information in real time."

SUPPLIER MANAGEMENT ADVANTAGES

What's more the AT&T BusinessDirect Portfolio delivers supplier management advantages that position a company to:

· Make cost saving business decisions, backed by critical AT&T networking performance data.
· Proactively address changing business conditions by re-routing toll-free calls and bringing voice trunks in and out of service.
· Launch circuit tests, check network alarms, and report service interruptions, without the time-consuming call screening.
· Deploy disaster recovery plans within minutes.
· Review, analyze and pay your bills, place orders, check current inventory, and more —with online convenience.
· Manage your AT&T network 24x7

For more on how AT&T can help your company, visit www.att.com/business

AT&T

---

far more secure and robust than the enterprise's. In-house IT staff is free to concentrate on the application itself.

• **Customizing depth-of-service.** Using managed services enables organizations to vary their depth of services by application or line of business. Outsourcing the management of a particular part of an application infrastructure provides end-to-end service—from a communications link and the hardware and software at either end of the link to installation, monitoring, and management services. Fees are based on performance and capability; the effect is to transform several chunks of a network into one, supported via a single point of contact. **sd**

recovery & continuity

Building the Survivable Network

FOR MOST BUSINESSES, THE COSTS OF downtime are truly staggering. A January 2004 survey from PriceWaterhouseCoopers shows that a company with $500 million in revenue could lose more than $4 million annually because computer downtime wrecks productivity. You need more specific numbers? According to Faulkner Information Services, a retail brokerage would lose $6.45 million per hour of downtime; for a credit card sales authorization outfit, the pricetag would be $2.6 million per hour.

If this sounds bad, it is. And most CIOs don't want to know: Indications are mounting that too many organizations have been too optimistic for too long about just how bad it can get.

- Nearly a third of organizations have no manual alternatives to their digitized data and processes, according to Gartner Datapro.
- A third of companies say they'll lose data or operational

THE THREE R'S OF SURVIVABILITY

RESISTANCE: The ability to deter attacks/failures

RECOGNITION: The ability to recognize attacks/failures and assess damage

RECOVERY: The ability to provide essential services and assets during an attack/failure and recover full services afterward

efficiency in the event of disaster because of insufficient planning and investment in business continuity, reports the Economist Intelligence Unit.
- According to Meta Group, just 20 percent of Global 2000 organizations have business continuity plans effective enough to provide a strong likelihood of surviving a disaster without lasting adverse impacts.

SECURITY POLICIES THAT WORK

"Unless policies meet business needs and are up to date and enforced, they will fail," says Christian Byrnes, vice president and service director at META Group.

To get ahead of the vulnerability curve, more and more organizations are using automated tools to help manage enterprisewide security policies.

After using Solsoft, Inc.'s Policy Server security policy management solution, France's premier press distribution company, Nouvelles Messageries de la Presse Parisienne, cut its security update process from two full days to 30 minutes. Policy Server flexibly supports NAT, VPN, and firewalls in the same package so organizations can improve security using their current technology and with minimal migration effort.

Using these kinds of tools helps IT staff keep networks, systems, and application in compliance with established security policies, helps reduce vulnerability to attack and thus lower incidence response costs, and makes it easier to adjust both policy and compliance efforts to changing business conditions.

The survivability imperative

BUSINESS CONTINUITY IS ABOUT SURVIVABILITY, the ability of a system (and those supporting it) to fulfill its mission in a timely manner despite the impacts of disastrous events.

As demand—from customers, employees, shareholders, suppliers, and regulators—for continuous operations intensifies, business processes and the applications and information that support them are becoming increasingly digital, increasingly automated, increasingly accessible via public networks, and increasingly vulnerable to the vagaries of complexity: failure, accident, and attack.

Thus, business continuity planning and development and deployment of the policies and technologies of survivability have become an imperative.

The good news: A well-developed business continuity plan can lower your organization's insurance premiums. Begin with an assessment that:

- Delineates the costs of disruption to normal business operations.
- Pinpoints critical business functions, operations, facilities and departments, and then defines the continuity requirements of their associated systems, networks, facilities, and personnel. **sd**

FOUR QUESTIONS THAT COULD SAVE YOUR COMPANY

If you want effective business continuity planning, start by honestly answering the following questions:

What essential services must survive attack/failure? Have you determined which of your business processes are business critical, which are mission-critical and cannot tolerate unavailability or data loss?

What affect will attack/failure have on the company? What will downtime or total business failure actually cost the organization? What is your mitigation strategy should those events occur?

What changes in architecture, processes and requirements can improve survivability? Are your key locations hardened? Have you established availability and security service levels with partners, customers? Are you able to comply with current and forthcoming laws and regulations?

Which changes offer the best payoff? Have you generated solid business rationales to support your risk mitigation investment choices?