NetworkWorld

Security White Paper Sponsors

To get a hard copy of the 16-page white paper mailed to you, please email Jane Weissman at JWeissma@nww.com.

Click on a logo below for more information at our sponsors' web sites.

F5 NETWORKS

Shavlik TECHNOLOGIES

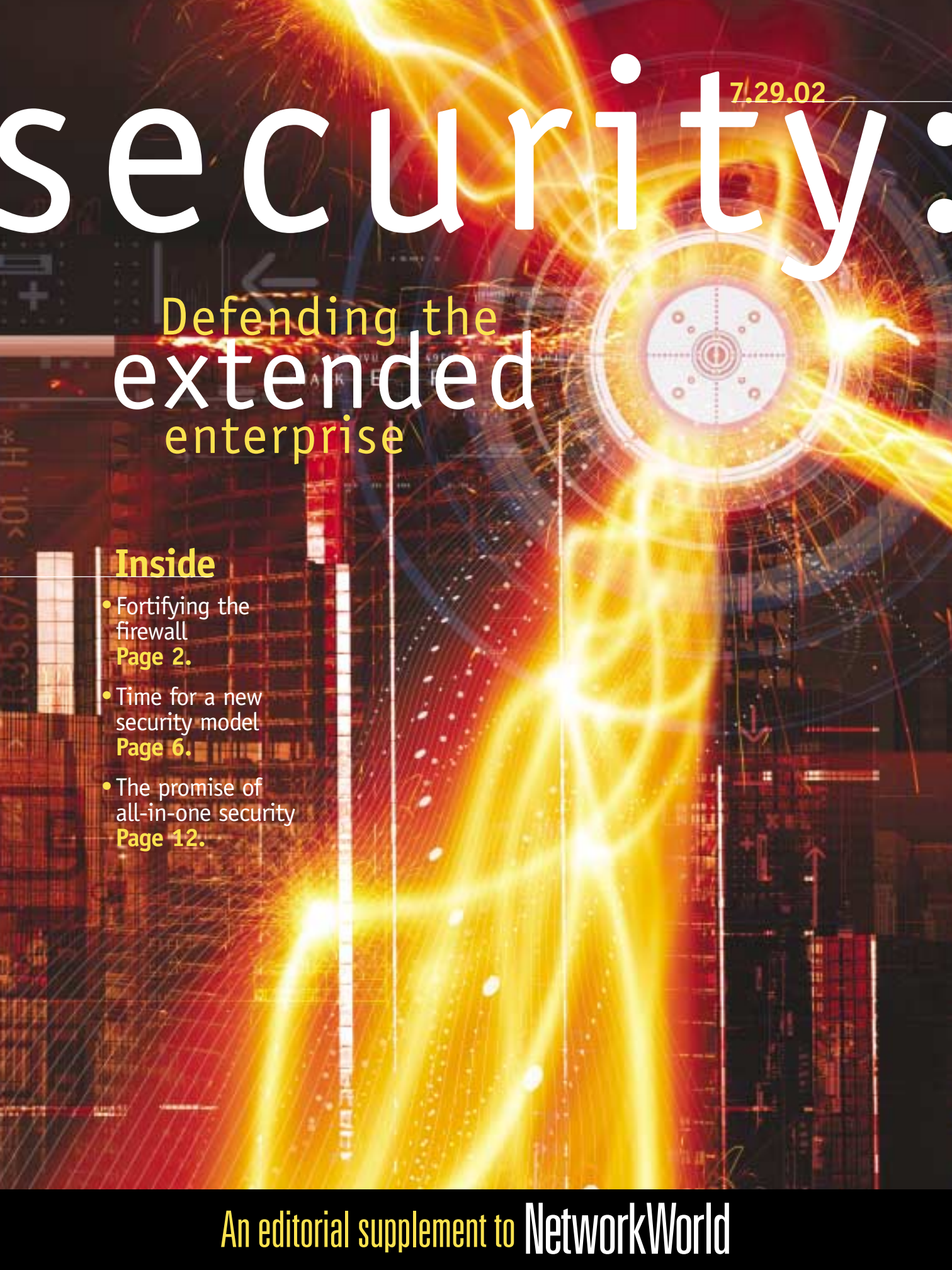
NORTEL NETWORKS

INTERNET SECURITY SYSTEMS

Top Layer

ZONE LABS

ca Computer Associates



security:

7.29.02

Defending the extended enterprise

Inside

- Fortifying the firewall **Page 2.**
- Time for a new security model **Page 6.**
- The promise of all-in-one security **Page 12.**

An editorial supplement to NetworkWorld

Fortifying the

Today's world of open network access means rethinking the role of the firewall.

By Bob Violino

Obviously, the firewall can no longer stand alone against all nasty intrusions. The chances that a virus or other ill-intended probe will penetrate a company's firewall rises almost daily, especially when ports are opened to give people outside the physical perimeter access.

Not that most network executives can even define the perimeter any longer. The distinction between what's inside and outside the corporate realm has vanished. In its stead has come modified perimeter architectures, built using more advanced firewalls that follow tenets of a security model for today's realities (see related story, page 6).

When network managers began deploying firewalls as security tools a decade ago, they could easily define the network perimeter. Most people who

Mirrored firewalls provide some comfort to Don Hoffman, who watches over The Mony Group's extended enterprise network as director of IT security.

PHOTO: MICHAEL GREENLAR

firewall

had access to corporate networks worked on desktop computers in the main office; external links to business partners were virtually nonexistent. A simple firewall-based demilitarized zone between the private and public network made sense. But today's practice of allowing access to corporate data to anyone who might need it — mobile workers, telecommuters, business partners, suppliers — from wherever they are over wired or wireless links turns that sensible decision into a foolish one.

To provide a high level of access, companies punch holes through the firewall barrier and hide data from the firewall's view by using technologies such as VPNs and encryption. This cripples firewalls — as they were originally designed — and keeps them from protecting companies against attacks, high-tech vandalism, theft of data or other security breaches.

On the attack

Data from the Computer Security Institute (CSI) shows the number of security breaches, already high, has grown in the past year. CSI's 2002 Computer Crime and Security Survey, released in April, indicates that 90% of the 503 participating U.S. organizations detected computer security breaches within the previous 12 months, up from 85% in the previous year. Eighty percent of the organizations said they suffered financial losses because of computer breaches, up from 64% the year before.

About 75% of survey respondents said their Internet connection was a frequent point of attack, compared with 33% who cited their internal systems as such. Forty percent detected system penetration from the outside, 85% detected computer viruses and 70% of those attacked reported vandalism.

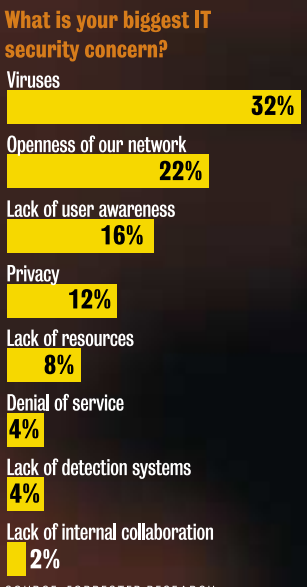
"Companies need to provide a lot of access to their partners, customers and employees today, and they're using technologies like Web services and extranets more frequently. All of this points to the fact that perimeter security by itself is no longer adequate," says Laura Koetzle, security analyst with Forrester Research.

"Businesses need to have firewalls, but there must be various layers of firewalls as well as clear policies that determine how these firewalls interact," Koetzle says. "Having nothing protecting the middle of the enterprise is a sure way to let someone come in and do maximum damage."

In a survey of 50 IT managers conducted by Forrester earlier this year, "openness of our network" was the second most common response given (after viruses) when managers were asked to name their biggest IT security concern.

Too many holes

The openness of corporate networks — i.e., firewall-based perimeters riddled with holes —is causing serious concern for IT managers.



On the defense

Firewall vendors such as Check Point Software, CyberGuard, Network Associates, Secure Computing and Symantec are trying to address the needs of increasingly open networks by bolstering firewall capabilities. For example, they are developing directory-based firewalls that issue access rights after a user has logged in and logical firewalls that separate groups within an organization. Other initiatives include:

- Designing firewalls to work more easily with intrusion-detection systems and antivirus software, or embedding those capabilities in firewalls.
- Offering firewall protection for equipment such as home office computers and wireless handheld devices.
- Providing firewalls that are embedded in components such as network cards, so individual devices on a network can be protected against internal and external threats.
- Offering filtering levels so firewalls can better determine the threat of specific messages or applications being sent.

Network executives taking advantage of new ways to design firewall -based perimeters are experiencing good results. The Mony Group, an insurance and financial services firm in New York, has installed mirrored firewalls to protect its perimeter. If one firewall fails, another stands in the way and ensures protection, says Don Hoffman, director of IT security.

"This makes us less vulnerable if we're attacked," Hoffman

says. "It used to be there was a single point of failure."

Still, Hoffman pressures firewall vendors to do a better job of getting fixes out when weaknesses in firewalls are exploited or when new threats emerge such as logic bombs or spam. "That's an underlying issue with security. We know a vulnerability exists, but we have to wait for the patches or upgrades," he says, adding, however, that vendors are improving. "They used to be a week behind the problems and now they're two or three days behind."

Despite growing sophistication, firewalls aren't enough, Hoffman says. Mony also uses VPN, IDS, authentication and other technologies to secure its corporate network. Plus, Mony is exploring whether internal firewalls would be useful in protecting particular departments and even individual devices.

Of course new firewall technology is only a partial solution. Policies must also be created. OSG Tap & Die, a tools manufacturer in Glendale Heights, Ill., uses Secure Computing's SideWinder firewall with a built-in VPN to connect via the Internet with its parent company in Japan, offices in Europe, and to selectively provide data access to workers in the field.

"When a salesman working in a hotel room needs to get access, he can come in through the firewall using the client VPN and I [can verify] he's actually the salesman through authentication," says Mike McKenna, IS manager at OSG.

However, McKenna is cautious about granting employee requests to transfer data to and from Web sites blocked by the firewall. "The Swiss cheese effect comes into play where you're creating holes in the firewall," he says. "We can't just make random changes in the firewall to accommodate all the requests."

New policies really come down to common sense, says Tom Warfield, systems administrator in charge of networking at government contractor AST in Lawton, Okla.

"We have a simple rule, if you're not using something, shut it off," he says. It might sound obvious, but "people tend to leave everything — desktop computers, laptops or other systems — turned on," and that invites trouble that the firewall can't always block.

Violino is a freelance writer covering business and technology. He can be reached at bviolino @optonline.net.

> "The **Swiss cheese effect** comes into play where you're creating holes in the firewall. We can't just make random changes in the firewall to accommodate all the requests."
>
> — Mike McKenna, IS manager, OSG Tap & Die

Firewalls and then some

With firewalls no longer able to be a solitary guardian against all potential threats, network executives "need to look at different ways to take the load off the firewall," says Don Hoffman, director of IT security at The Mony Group, an insurance and financial services firm in New York.

Hoffman says Mony is using technology such as IDSs at the front and back ends of its firewall to help control access to internal networks and data. He says most firewall vendors will soon begin building intrusion-detection capabilities into their products, if they're not already (see related story, page 12).

RICHARD BORGE

Firewall vendors must work with other security product developers to integrate their products, says Tom Warfield, systems administrator who's in charge of networking at government contractor AST in Lawton, Okla. Warfield likes that his firewall supplier, Check Point Software, does so. "Check Point has allowed other vendors to integrate their products into the firewall, and it ensures that these products meet industry standards and certification," Warfield says. He cites one such partnership, which integrates Symantec's Norton AntiVirus products with Check Point's Firewall-1.

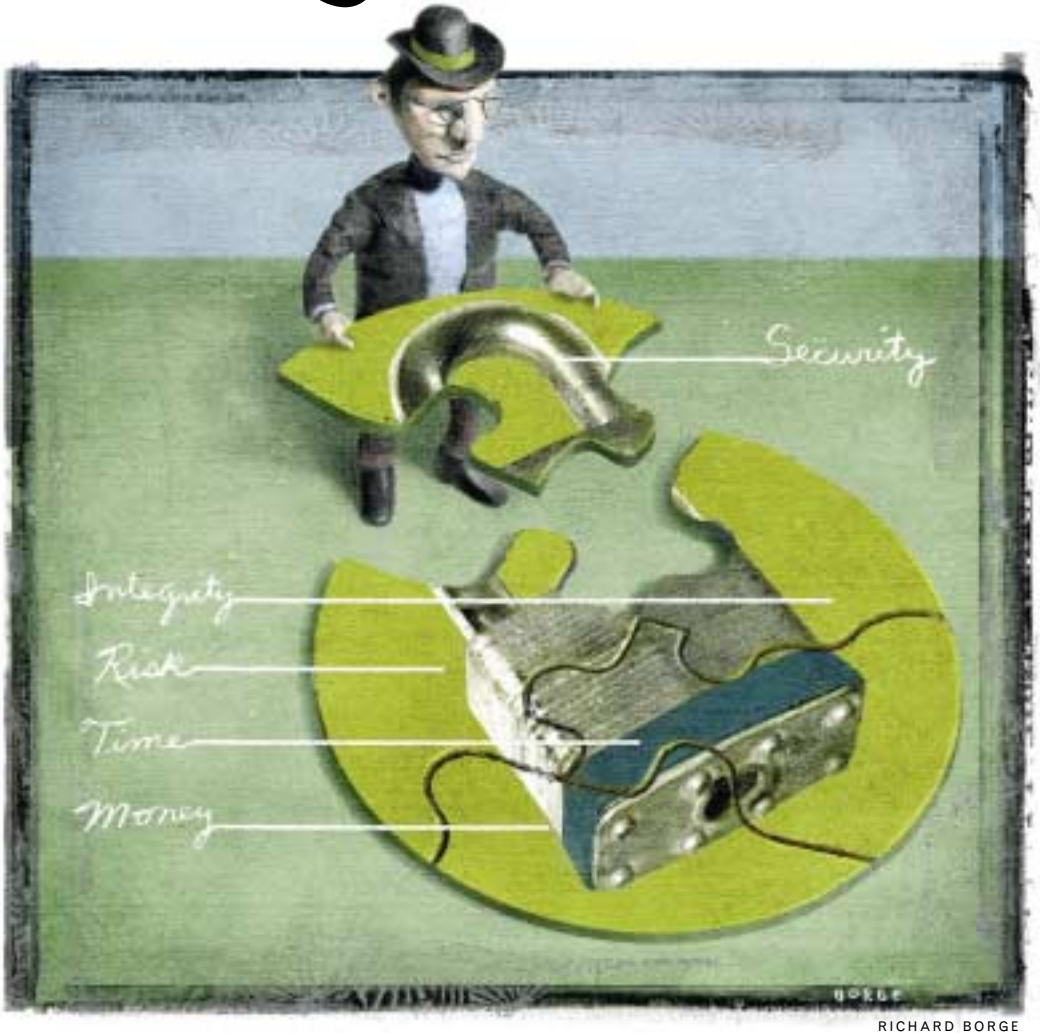
"The Norton software works well with our firewall," Warfield says. "In the past we had a lot of problems with people downloading viruses that spread through the company." The firewall/antivirus combination has been an effective solution, he says.

— Bob Violino

Time for a new security model

The classic goal-oriented model for security design is broken. Fixing it will require new attitudes toward security planning.

By Julie Bort



RICHARD BORGE

Confidentiality, integrity, availability: The security industry declares these the goals of computer security. While this goal-oriented approach to defining security needs, known to security folk as the "CIA model," is good as far as it goes, it no longer goes far enough.

Forged in the early days of the Internet's commercialization, the classic CIA approach took on authentication, access control and nonrepudiation as goals in the mid-1990s. Since then, this model has become standard security fare.

But the goal-oriented approach neglects today's critical security needs, where attacks are more sophisticated, frequent and from a wider range of sources. For instance, the traditional architecture for implementing the CIA model — the firewall-based perimeter — is increasingly ineffective.

Worse still, the goal-oriented approach does nothing for the other half of good security planning: risk assessment. Risk assessment, which guides security managers in prioritizing security

spending, is sorely neglected even in organizations that acknowledge its importance.

"We use CIA as a guideline, but the majority of what we do now is a 'disaster-recovery' model. What can we live without, and what is the impact of without? But our company unfortunately has not done a lot of risk assessment — only to say, if we lost it, what does it hurt?" says a senior network security engineer for a global, Fortune 100 food corporation who asked not to be named.

Despite these shortcomings, the security industry and users overwhelmingly assume that CIA is the best way to achieve high security. Network executives can't afford to buy into that assumption. True, confidentiality and its five siblings forever will be security goals. Yet goals are only a portion of the plan. Other portions should be risk assessment and a modified version of the "tried and true" demilitarized zone (DMZ) perimeter. Critical, too, is the need to recognize new goals as they emerge.

Time will tell

CIA thinking has turned security planning into a product game. Security equals the installation of point products that perform goal-oriented tasks. You install encryption for your confidentiality, tokens for your authentication, firewalls for your access control, and so on. If a failure occurs, the theory goes, execution is to blame (a missed patch or faulty setup), not the underlying design.

But chasing after goals with products is a flawed tactic on several counts. It can lead to times when the goal is achieved but security isn't. For instance, 128-bit key encryption will endow critical e-mails with confidentiality, and maybe integrity, but it won't stop a worm at the ISP from munching messages before recipients read them. So while the security goals for messages were met, the business goal of ensuring safe delivery of critical information was not.

Basing security on achieving goals sets you up for failure because it requires always-perfect product implementations (not a real-world expectation), or at least one back-up system for every product (not fiscally feasible or responsible).

Far wiser is basing your security architecture on an acceptable percentage of time goals should be met, which is what risk assessment tells you. If you know how much money a specific breach will cost the company, you can determine the acceptable percentage of time a security goal can be missed and how much to spend on defense.

This risk assessment will let you conquer what users say is security's biggest hurdle: obtaining adequate budgets.

"Security is a hard sell because if I'm doing my job right, nothing happens," says Matt Raymond, manager of information security for employment agency Robert Half International, in Pleasanton, Calif.

Risk assessments often are neglected because network executives are typically technology specialists, not risk analysts. One model that simplifies the task is time-based security, says its developer Winn Schwartau, security consultant, author and *Network World's* "On Security" columnist.

Time-based security lets security managers "mathematically quantify" security risk, Schwartau says. It assumes the worst-case scenario — no security — and calculates how much damage could be done in the time it takes a company to detect a hack and react to stop it.

"With a jewelry store, a thief could easily breach security — just hammer through the window. But that triggers an alarm. How much a thief can steal in the time it takes the police to get there is the risk," Schwartau says. "Detection plus reaction equals risk. This is identical in the cyberworld." The trick is assessing the value of the stolen data, he adds.

When following this model, security executives determine which files could be accessed in a specified amount of time, such as the four days Schwartau says it typically takes to realize a breach.

Dividing file size by bandwidth will pinpoint the amount of time a hacker would need to grab that file and, therefore, which files are at risk. Myriad other formulas give security managers other measurements of risk, which they can turn over to risk-assessment specialists. Those specialists can determine the value of that data (a research and development database or customer billing information) and what it's worth to secure.

And that, users say, is the Holy Grail. "Executives recognize that things need to be done for computer security but don't have a real understanding of what the computer systems do. I need to present it to them in actuarial tables — the way they understand," the senior network security engineer says.

No more Tootsie Pops

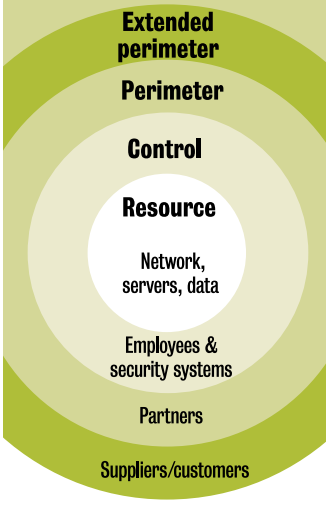
Network executives must also revise their traditional models of implementation, says Howard

"Security is a hard sell because if I'm doing my job right, nothing happens."

— Matt Raymond, manager of information security for Robert Half International

Security in layers

Burton Group's "Virtual Extended Network" model is an alternative to traditional demilitarized zones. Its four layers represent security techniques for different zones of use.



More online!

Cybersecurity legislation: What you need to know.

DocFinder: 1430

Schmidt, vice chairman of the Critical Infrastructure Protection Board, an advisory board to the federal government on national IT security defenses. This means overhauling the traditional DMZ design.

"I call it the Tootsie Pop syndrome — hard outer shell/soft chewy center. The traditional way we look at network security is to create the firewalls and environment to keep people out. But once someone is inside, he can pretty much do what he wants," Schmidt says.

Rather, network executives should concentrate on securing all pieces of the network puzzle — clients, wires, servers and applications, Schmidt says.

But securing every PC and node individually can create a support nightmare, users say, particularly in companies with thousands of them, in hundreds of offices across half a dozen countries.

The new Virtual Enterprise Network (VEN) security model, created by research firm Burton Group, offers a compromise.

"The hard-shell/soft-chewy center model no longer works in an era of virtual enterprises," contends Daniel Blum, Burton's senior vice president and research director and *Network World* "Intranet Advisor" columnist. "VEN is a layered defense."

Specifically, the VEN model defines four logical layers: the resource layer, which houses clients, servers, applications and data; the perimeter layer, which defines an organization's physical boundaries and contains firewalls, proxies and gateways; the control layer, where authentication services reside as do controls for security policies across layers; and the extended perimeter, where companies engage technologies or services to secure resources physically located outside the perimeter.

The upshot is a model that builds on the existing infrastructure, but plans for a distributed perimeter, Blum says.

Missing the goal

While goals might not be an appropriate basis for your entire security model, they remain an important part of security planning. But you shouldn't be able to count off the whole list on one hand. One addition should be the protection of a company's reputation, Schmidt says.

Users agree. "If you have a Web site and all of a sudden someone's selling all of your [customer] names off your site, or they end up putting their name on your Web site, your reputation will be damaged," Robert Half's Raymond says.

Likewise, brand protection also needs to be a security goal, say Schmidt and other experts.

Taken together, a top-notch risk assessment, revised DMZ implementation and expanded goals make for complete computer security today. Yet this plan is only one leg of the three-legged cybersecurity table. The other two are physical security and trustworthy people, Schwartau says.

A company's maintenance or building security staff traditionally has handled building access and other physical security systems, without input from security professionals in IT. That needs to change so that the swipe of a building-access card is not a stand-alone event, Schwartau says.

"That [building-access card] database should talk to the other databases and say, 'Hey, how come Bill is logged into his machine if he wasn't in the building?'" he says.

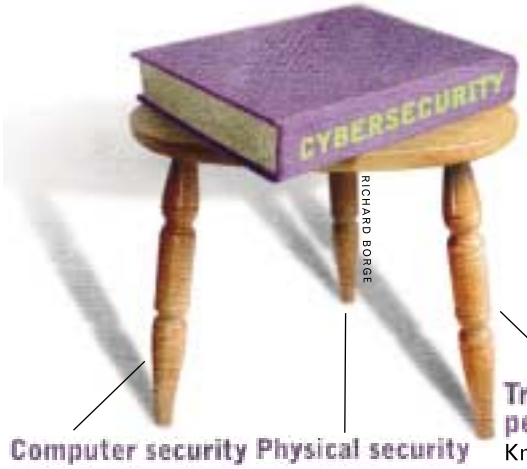
As for people, Schwartau and Schmidt make two points. The first is that all the technology in the world won't help if your people don't follow your processes for auditing, patch maintenance and other ongoing support. The second is that you should verify the trustworthiness of anyone to whom you will be giving significant network access by running background checks. This is particularly important when hiring IT contract workers in countries known to harbor terrorists, Schwartau says.

Strong IT security can only be accomplished if all of the table legs are equally sturdy. ■

> "Traditional . . . network security is to create the firewalls and environment to **keep people out**. But once someone is inside, they can pretty much do what they want."
>
> — Howard Schmidt, vice chairman of the Critical Infrastructure Protection Board

The three legs of security

In this age of terrorism and sophisticated cyber threats, business security rests upon a three-legged defense.



Computer security
Use risk assessment, CIA+ new goals, and extended enterprise planning models.

Physical security
Integrate physical access systems with network authorization systems.

Trustworthy people
Know who you give access to. Avoid consultants from countries that harbor terrorists.

NetworkWorld

Editorial Director: John Gallant
Editor in Chief: John Dix

Supplements
Editor: Beth Schultz, *(773) 283-0213;*
Fax: (773) 283-0214
Executive Editor: Julie Bort *(970) 468-2864;*
Fax: (970) 468-2348
Art Director: Tom Norton
Graphic Designer: Jacy Edelman
Online Graphic Designer: Zach Sullivan
Copy Editor: Greg Cusack

The promise of all-in-one security

The lure of simplicity is prompting users to consider bundled security products. By Jennifer Jones

At least three times per week, Arkansas State University's network is threatened by a virus, denial-of-service attack or system hack, often by students trying to tap the school's resources from their dorm rooms.

"The reality is my network is my own worst enemy," says Greg Williamson, associate IT director at the Jonesboro school.

The university relies on multitasking devices to stave off such attacks. Arkansas State uses four Cisco Catalyst 6513 Gigabit Ethernet switches outfitted with intrusion-detection system (IDS) modules. IDS belongs squarely in the network's core, Williamson says.

"If the core goes down, so does the network. With voice over IP running on the network to serve resident housing, there is a high-level, critical need for 911 services. The network can't go down," he says.

Greg Williamson, associate IT director, stands guard over the Arkansas State University network with the help of IDS blades in backbone switches.

STEVE JONES

The IDS blades watch traffic as it crosses the switch backplanes, defending against denial-of-service and other attacks, Williamson says. They simultaneously monitor multiple virtual LANs. If a blade detects malicious or unauthorized activity, it triggers an alarm.

Injecting security functions into network gear like routers and switches is one method of integrated security attracting the attention of enterprise network managers. Another is tools that blend two or more security functions, such as IDS, Internet filtering, firewall, vulnerability assessment, and virus scanning. Vendors also are embedding security features into nonsecurity software products, such as virus scanning into e-mail.

The lure of simplification

In a traditional network security setup, each device — firewall, IDS and vulnerability assessment tool — has its own console. Bundled products promise to integrate these, an appealing prospect to users.

"The benefits of using integrated solutions to us would be the use of a single management console to manage different security layers," says Aidan Garcia, network services manager at Eastern Bank in Boston.

Mike Cothren, MIS director at the Pulaski County Special School District in Little Rock, Ark., says simplification was a

reason his organization chose appliance vendor SonicWall, which supplies the district with the SonicWall Global Management System. Along with firewall capabilities, this appliance performs Internet filtering by checking each request sent from Pulaski's LAN against a list of unacceptable URLs and IP addresses. It denies requests deemed inappropriate.

"Trying to make products from different vendors work together can be a nightmare. If there is a problem, each vendor will point its finger at the other. This allows you to work with one tech support shop that will handle all the issues," Cothren says.

Integrated products also could eliminate duplicate security functions and lower false-positive alarms — incidents in which systems report problems that have not occurred.

"One of the things integrated vendors claim is that their products will have people spending less time on worthless administrative things and more time on critical threats," says Chris Christensen, an analyst with IDC.

To that end, vendors have unleashed a wide variety of integrated security products.

TippingPoint Technologies, for instance, hawks a combined firewall/IDS device the company says can outperform software-based offerings and costs less because it is part of the network infrastructure.

NetScreen Technologies says it soon will support IDS and virus scanning on high-speed devices already hosting firewall and VPN software. NetScreen's offering "certainly would be an attractive thing," says Chuck Horvat, director of network services at Divine, a service provider in Chicago using integrated NetScreen appliances at all 27 of its corporate infrastructure sites.

Along those lines, Nokia and Internet Security Systems (ISS) allied last year on RealSecure for Nokia, an IDS appliance the vendors say will build on Nokia's firewall capabilities.

Other alliances include a Network Associates and ISS agreement that pairs McAfee antivirus technology with ISS' RealSecure IDS products.

SonicWall user Pulaski County will benefit from a similar partnering because the organization is poised to implement McAfee antivirus capabilities on the SonicWall platform.

"The solutions we looked at generally would require a Windows 2000 server to manage virus updates to the workstations," Cothren says.

Because the school district is a Novell shop, adding the Microsoft servers would have added cost and complexity that Cothren preferred to avoid, he says.

Meanwhile, Inktomi announced in April that it had combined virus scanning, content filtering, user authentication and access controls into its caching software, Traffic Edge Security Edition.

In contrast to product bundling, Crossbeam bills Version 2.0 of its X40S appliance as a common platform for running applications from leading security vendors, such as Enterasys Networks' Dragon Sensor IDS and Check Point Software's firewall and VPN software. The company suggests the device can stand in place of servers, load balancers and switches.

E-mail vendors are also nailing down security alliances. Rockliffe teamed with F-Secure to inject virus scanning into Version 5 of its MailSite SE software.

Watch for laptop and mobile devices to join the crowd, too, by adding authentication like tokens or biometrics.

A hybrid approach

But for all the promise and vendor activity, integrated products have a spate of potential drawbacks. For instance, IDS, a commonly bundled technology, is difficult to engineer. (Visit www.nwfusion.com, DocFinder: 1431, for related story.) And users like Eastern Bank's Garcia who yearn for easier management worry that a bundled product creates vulnerability.

"The shortcoming that has prevented us from investigating integrated solutions has been the single point of monitoring. If hackers could find a way around the system, they would have open access to the network beyond it," he says.

For such reasons, analysts question how widely enterprise users will accept bundled security wares. Eastern Bank has decided to forgo them for now. It stitches together dedicated products from vendors like Network Associates, Garcia says. Eastern Bank uses McAfee virus protection suite and e-business server.

A hybrid approach, using both dedicated and integrated products, makes sense even to Arkansas State's Williamson, an avowed believer in integrated security tools. "It has to be blended at this point," he says, characterizing the university's planned security architecture. "But while the integrated pieces seem to work better for us in many situations, I am still buying separate appliances as well."

The university employs several stand-alone IDS appliances to monitor traffic passing through switches and uses firewalls at the network perimeter and in a server farm, he says.

"I can't look at a single security appliance or integrated appliance and rest knowing that it will protect me," says Williamson, who says that the university's ongoing VoIP upgrade makes security even more vital.

"We are putting in 100M-bit/sec connections to potentially hundreds of hackers sitting in their dorm rooms," he says. "I'm not going to put all my eggs in one basket."

Jones is a freelance writer in Vienna, Va. She can be reached at jjwriterva@aol.com.

All-in-one packages

Here is a sampling of wares that combine security functions traditionally provided in separate devices.

Vendor	Product
Cisco	Catalyst 6000 switch family with intrusion-detection system module
Crossbeam Systems	X40S Open Security Appliance
Inktomi	Traffic Edge Security Edition
NetScreen Technologies	NetScreen series appliances
Nokia	Nokia IP Security platforms
SonicWall	SonicWall Internet security appliances
TippingPoint Technologies	UnityOne Network-Defense Systems

More online!

- Hope for IDS. **DocFinder: 1428**
- Users mistrust bundled security. **DocFinder: 1429**

www.nwfusion.com