

# The Security Pros Talk

10 tips from veteran Sun Certified Providers who reveal practical strategies for keeping your network secure

**D**espite daily headlines reporting security breaches at major corporations, most businesses have no clue how vulnerable their networks are. Only one in seven companies has bothered to develop a basic security policy. Therefore, it's not surprising that hackers continue to exploit well-publicized loopholes in software, and that workers unknowingly usher viruses through their company's firewall.

"Organizations spend very little time understanding their risks and vulnerabilities," said Russel Sanders, Business Solutions Engineer for Dewpoint, Lansing, Mich. "They really give themselves a false sense of security."

Sun Microsystems Certified Providers have a huge library of practical experience in solving the most vexing security challenges. They help companies understand their security requirements; guide them in choosing the right technology; help develop policies that balance the conflicting demands of security and usability; and monitor companies to make sure they adhere to the policies they have set.



Here are 10 recommendations from these battle-scarred experts that will help you make your enterprise—and your business—more secure:

## *Harden Your PBX System*

Many companies now integrate their PBX systems into the TCP/IP network for easier administration and maintenance. Often, however, those companies forget to equip the PBX with firewalls and filtering software that limit access through the use of strong authentication. At the very least, the PBX system should be disconnected from the Internet until maintenance of the PBX is required.

"The PBX doesn't get a lot of attention in the media, so it's often overlooked," said Kelly Dowell, CEO of Garrison Technologies, Austin, Texas. And the IT department often

doesn't have control over the PBX and simply forgets to consult with the telecommunications department, which often is much less knowledgeable or concerned about network security issues.

A compromised PBX system can expose a company's voice mail and conference calls to prying ears, as well as make a company vulnerable to toll fraud. Dowell said Garrison once audited a company that hadn't secured its PBX system and found that an employee had breached the system to set up 800 numbers that he, his mother and girlfriend had been using for a year at the company's expense.

### *Close Holes When You're Done*

It happens everyday—an engineer needs a one-to-one connection so that a vendor can pull information off the engineer's system to debug a problem. "The next day the engineer tells IT he needs the connection open for another 24 hours, because he's still having problems," said Steve Kwan, director of professional services at Ignyte Technology Inc., Santa Clara, Calif. "Eventually, people just forget to close up the port."

Companies need to develop rigid policies and exercise discipline to ensure that holes stay closed. For example, if a bank needs to receive a feed from a third-party service provider, the bank shouldn't automatically open a port for them. "There should be a specific policy for how that provider connects, using a VPN or a configuration to a specific address," said Garrison Technologies' Dowell. "Don't give providers continuous free access to an open port—require them to call in so you will open the port for them."

Every company has valid reasons to open holes in firewalls, but those openings should have a clearly defined life expectancy. "And each company should conduct a quarterly or semiannual firewall rule review," said Charles Rawls, senior director of systems and networking at Thaumaturgix in New York.

### *Change Passwords On The Systems And Backup Account*

Sure, you can force users, some with limited access rights, to change their passwords every 30 days, but that doesn't address a larger problem: Many companies retain the same systems passwords for years, a bad move because it fails to protect the system from people who have left the company but can still access the network because they know the password.

"Or, a systems IT manager will have his or her user name as a password with full administrative rights," said Jeff Stark, Co-founder and President of Ignyte Technology. But when the IT manager goes to another company, no one changes the password or the password on the backup account. "If you don't go through the time-consuming process of changing the passwords and making sure the backups work, you could be leaving huge holes," Stark said.

### *"Love" Isn't All You Need*

Don't use easily guessable passwords, such as "love," "money" or "wizard," advised Sanders of Dewpoint. All companies need a password policy that details user responsibilities and verifies password quality. This policy should insist that all default passwords be changed before a machine is connected to the Internet. "The Sun Solaris™ operating system provides some administrative tools that allow you to specify things such as password length, days between changes, and uniqueness which are all strictly enforced at the operating system level," Sanders notes. "Additionally the OS requires at least two alpha characters and one numeric or special character in addition to a minimum length of six characters."

### *Keep Current With*

#### *Manufacturer-Supplied Security Patches*

Thaumaturgix's Rawls instructs junior security analysts to regularly track industry and vendor advisory forums. "Sun Microsystems is particularly good with recommended patches," Rawls said. "A lot of companies don't apply the patches because they don't want to mess with a working system, but this can leave their systems at risk." So can simply doing patches once every six months—which leaves an operating system in need of a patch exposed to intrusion for months. Remember, hackers read forum advisories, too, looking for new vulnerabilities to exploit.

### *Monitor Remote Users*

Employees dialing into the network from home or the road on an unsecured cable modem or DSL line present huge security risks. Currently the only way companies can protect themselves is to inform remote users to never leave their home computers on or unattended if they have a virtual private network. "The big challenge now is that host-based security has to be centrally managed and cannot be run by the remote user," Stark said. "They'll just turn it off or configure it incorrectly."

PGP Security, a Santa Clara, Calif.-based division of Network Associates Inc, has just released PGP Desktop Security 7.0, a mobile security device that handles this problem. Desktop Security 7.0 combines a personal firewall, personal intrusion detection, VPN secure connectivity and enterprise-class manageability, so IT can make sure remote workers' connections are locked down.

Mike Wallach, president of PGP Security, expects this trend to move inside—with companies realizing they need client-based security for internal users as well as those connecting to the network from the outside.



### Take Sample CGI Programs Off Production Servers

Many Web servers include sample common gateway interface (CGI) programs, which make Web pages interactive. There's a problem, though: CGI programs are easy to locate and have the privilege of access to the Web server software itself. "If a hacker subverts one poorly written CGI script, that hacker subverts the firewall and has complete access to the network," Garrison Technologies' Dowell said. "Scanners won't catch that because CGI scanners can only look for known vulnerabilities, not proprietary code." One study blamed a CGI hole for a hack attack on the Department of Defense Web site, where someone swapped Janet Reno's photo with one of Adolph Hitler.

### Back Up The Firewall Configurations

Failing to do backups and test them is one of the most common security oversights, especially with regard to firewall configurations. Hardware fails. "You don't want to be running around trying to remember what the IP address on the firewall was," Thaumaturgix's Rawls said.

### Review Firewall Logs

Busy IT directors don't realize their logs contain information that can preempt some security problems. "If someone is going to try to beat up the network, the first place you'll see it is the firewall logs," Rawls said.

For anyone paying attention, these logs contain all sorts of unexpected and useful information, such as pinpointing internal users who are surfing hacker sites. "Security is not a firewall or an access list you put on a router," Ignyte's Stark said. "People have to monitor the whole process."

PGP's CyberCop Scanner provides security auditing and reporting features that make finding and closing known vulnerabilities a simple task for administrators. "It's important to have sensors with intelligent agents throughout the network and on the servers," Wallach said. "Otherwise, you have no way to know that the same person just typed a different password on the same server for the one-hundredth time."

### Make Sure Users At All Levels Understand What To Look For

So, you're congratulating yourself because you've briefed the top executives on proper security, and life is good. But what about the receptionist? "The receptionist should always be security aware," Rawls said. "The age-old hacker technique is to call, chat up the receptionist and, based on what he's learned, take a guess at user passwords."

Many security breaches occur because of basic human error or inattention to details. Often, workers are just too trusting. For example, employees will paste their passwords on yellow Post-It notes on their monitors—where everyone

can see. Or someone will call on the phone to ask that their password be changed, even though they are not authenticated. "Products such as token cards can prevent this, but training programs are needed throughout the company to teach and reinforce the value of good security," said a Sun Microsystems white paper called "Protecting From Within."

"People forget security is a business process," Dewpoint's Sanders said. "Over time, people become lax with passwords. And companies have a tendency to not grade data, so the user community doesn't know what security is required on a particular document."

Send e-mail messages and hold seminars to educate users on their security responsibilities. Your company could have the best technology in the world, but if employees don't know what to do when they encounter suspicious or threatening activities, your company could still be at risk. And in light of the consulting and technology resources that are available, that doesn't have to happen.

***This special advertising section has been sponsored by MOCA, Inc. The resellers featured are MOCA's customers and have a high level of expertise in the security area. To obtain additional information regarding the security solutions offered, go to [www.IIsolutioncenter.com](http://www.IIsolutioncenter.com)***

Sun, Sun Microsystems, the Sun logo, and Sun Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

***For information on Sun Microsystems and security solutions through a Sun Certified Provider call or e-mail:***

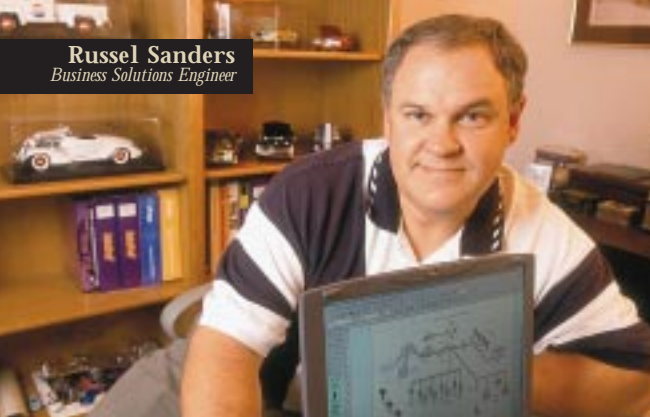
**Dewpoint**  
Russel Sanders, Business Solutions  
Engineer  
517-347-7800  
[rsanders@dewpoint.com](mailto:rsanders@dewpoint.com)

**Ignyte Technology**  
Frank Mong, Director of Marketing and  
Business Development  
1-877-5IGNYTE (1-877-544-6983)  
[frank.mong@ignyte.com](mailto:frank.mong@ignyte.com)

**Garrison Technologies**  
Ty Mellon, Director, North American Sales  
800-344-6309  
[sales@garrison.com](mailto:sales@garrison.com)

**Thaumaturgix**  
Randall Truesdale, Senior Technology  
Alliance Specialist  
212-972-2030 Ext. 5040  
[randall@tgix.com](mailto:randall@tgix.com)





## CUTTING LINKS, KEEPING SECURITY

Many companies want to cut out the middleman. But how can you do that without cutting out security as well?

A company that provides access to clients through a sales force of several thousand using direct dial-up network connections faced that very problem. Dewpoint was able to give end users control by deploying next-generation directory services from iPlanet E-Commerce Solutions, a Sun-Netscape Alliance. This tool allowed e-mail, calendar, e-commerce, ERP, supply-chain management and other applications and services to access LDAP directory functionality and use directory information through easy-to-use application programming interfaces.

"The external user is challenged for his name and password," said Russel Sanders, Business Solutions Engineer for Dewpoint, Lansing, Mich. "The agent on the Web server picks up the result of that challenge and forwards it internally to the authorization access device."

## Dewpoint

The key technical element of the solution is fault tolerance, leveraging the high availability of Sun servers. "In these projects, people often overlook load balancing," Sanders said. A centralized authority without redundant servers, services and paths could become wide open if the primary server were to fail. "High availability for security purposes means more than a redundant network connection to the server," Sanders said. "The applications themselves can be made redundant and work in harmony. When some systems fail, they leave a huge hole in the network."



Politics tends to be the biggest problem with a directory project. "Every department had its own directory architecture," Sanders said. "Does each department want the directory to be authoritative? Of course. Does it have all the information they need to host and protect enterprise security? No."

Dewpoint's role is to help "bring sanity" to the politics. Sanders assured the various departments they could retain their proprietary content. "We told them that with a centralized authority, when someone left the company we wouldn't have to change their passwords on 30 systems," he said. "We only had to change the password in the centralized point, and it would propagate to every system. That assuaged them."

[www.dewpoint.com](http://www.dewpoint.com)

## Garrison Technologies

### KEEPING ON TOP OF THE FIREWALL

Some companies run a few network scans that search for known vulnerabilities and call it "a security audit." But Garrison Technologies, an e-business security specialist in Austin, Texas, knows that a true security assessment must probe deeper into the networks, policies, and applications in order to provide maximum protection for a company's infrastructure. On one occasion, this diligence ended up providing improved security for the firewall industry as a whole.



Garrison had been performing a routine security assessment for a Seattle-based bank. "We found an open port on a server that was not identified as a risk by the initial scans," recalls Jim Stickley, Garrison's Director of Engineering. Stickley's team recreated the scenario in Garrison's lab in order to further analyze the issue.

What Stickley found was a flaw in the award-winning firewall, which is used by thousands of corporations, including many Fortune 100 Companies. The firewall contained a buffer overflow issue, exploitable externally from anywhere on the Internet. "Using this vulnerability, I could gain root access on the firewall, which means I could scan, attack and monitor the bank's entire network externally," Stickley said. "At the time, this flaw was considered theoretically impossible."



Garrison wrote a fix for the bank, and promptly alerted the manufacturer for resolution. "We found that problem through Garrison's comprehensive assessment methodology. Had we relied on a scanner, the vulnerability would have gone unnoticed," said Kelly Dowell, Garrison's CEO.

Security is an ongoing process, for both vendors and end users. Despite the continual stream of new vulnerabilities, Garrison professes strong security is attainable through current technology, proper planning, and maintenance. "There are numerous considerations in deploying these technologies successfully," said Dowell. "One, not to be taken lightly, is the reliability of the platforms on which they run. If the application goes down, so does the protection and, often, the network services," said Dowell. "Sun Microsystems servers provide us with the performance and reliability needed for our client's critical security applications."

[www.garrison.com](http://www.garrison.com)



**Jeff Stark**  
Co-founder and President

## Ignyte Technology

solutions has made them the de facto choice as the platform to support, manage and maintain our mission critical solutions.”

As part of Ignyte Secure Path, Ignyte keeps a support account manager (SAM) who advises Applicast’s sales team on-site. When Applicast is selling its ASP services, potential customers have plenty of security questions. “Our account manager is involved in the sales process when it comes to the questions of connectivity options and security issues,” Stark says.

The SAM also acts as a liaison between Applicast’s implementation services, and Ignyte’s 24 x 7 network operations center to develop a proactive support package for every implementation.

Ignyte leverages both its Secure Path Methodology and Applicast Implementation Support methodology to ensure highly reliable and secure network connectivity. This is attributed to a scaleable, flexible architecture that Ignyte and Applicast jointly developed to provide a seamless, predictable networking service to Applicast customers.

“Our security design, network operations center, support account managers, and design team allow ASPs like Applicast to concentrate on their core business of providing applications,” Stark says. “The ASPs do not have to figure out how to design, support and manage the myriad of technical, business, and operational issues that coincide with secure connectivity and network security management.”



### HOW OUTSOURCERS OUTSOURCE SECURITY

Applicast, a fast-growing Application Service Provider (ASP) in Menlo Park, California, offers full-service application outsourcing for mission-critical applications, such as SAP and Siebel, over secure private or Internet connections.

As a successful outsourcer, Applicast knows when it needs to turn to another outsourcer for security. Ignyte Technology, a management security services provider in Santa Clara, California, caters to the fast-growing (ASP) market. “The biggest challenge is that most ASPs haven’t devised a security policy from the top,” says Jeff Stark, Ignyte’s Co-founder and President. “They’re so focused on customer acquisition and growth that they lack the bandwidth to resolve some of the network security issues surrounding outsourcing applications.”

Ignyte provisions, installs, and manages on a 24 x 7 basis, the network security and connectivity between Applicast’s customers and the enterprise applications located at Applicast’s data centers. Ignyte leverages a monthly recurring billing model to parallel the application services provider pricing model. “We use Sun hardware and software as the foundation for many of the services required to make this solution work,” Stark says. “Sun’s leadership status in UNIX based technology

[www.ignyte.com](http://www.ignyte.com)

## Thaumatargix

### DON'T CREATE YOUR OWN BREACHES

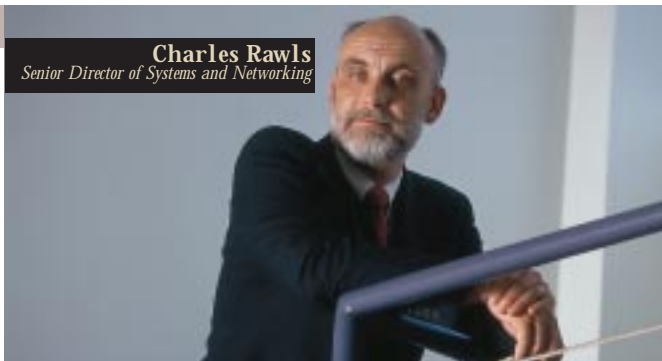
Charles Rawls, senior director of systems and networking for Thaumatargix Inc., a New York systems integrator, says many companies inadvertently create their own network security breaches while

searching for ways to make their operations more efficient. Many businesses open so many ports

to allow traffic through their firewalls that “they don’t have firewalls anymore—they have a router,” he said.

Thaumatargix audited one company that had run out of IP addresses in its development environment, a relatively common problem. The audit showed plenty of unused space was available on the demilitarized zone where servers are kept so people from outside the company could log onto test sites. There was a problem, though: “The DMZ is called the demilitarized zone because it’s much less protected,” Rawls said. “The rule set for the DMZ is much less strict than in a development or production environment.”

The company being audited hadn’t realized it had pushed critical information into an unprotected area. Almost anyone could log onto the mail server on the DMZ and read the system administrator’s e-mail detailing the new root passwords to everyone in the system in plain text. Rawls offered the company two solutions: allocate more IP address space to the development environment, or move to network address



**Charles Rawls**  
Senior Director of Systems and Networking

translation, which would eliminate address space requirements.

“On backing up firewall configs, we’ve regularly used an on-demand TFTP to backup Sun/Firewall-1 systems, logs get sent to a log host and perl scripts are used to locate entries of an interesting nature,” Rawls says. “The Sun/Firewall-1 combination is a wonderful high throughput system. I have used it in high traffic networks, and it has sustained its ability to filter traffic and keep the site running, under some determined denial of service attacks.”

Effective security mandates that companies scrutinize how every infrastructure change affects the network, architecture and security requirements. “If you want a nice easy solution to security, reach behind everyone’s computer and pull out the cord,” Rawls said. “But if you want a security solution that works for the business, you have to look a little harder.”

[www.tgix.com](http://www.tgix.com)