



# Security

Make a New Year's resolution to off-load everyday tasks and to spend time researching and implementing new technologies.  
BY MIKE FRATTO

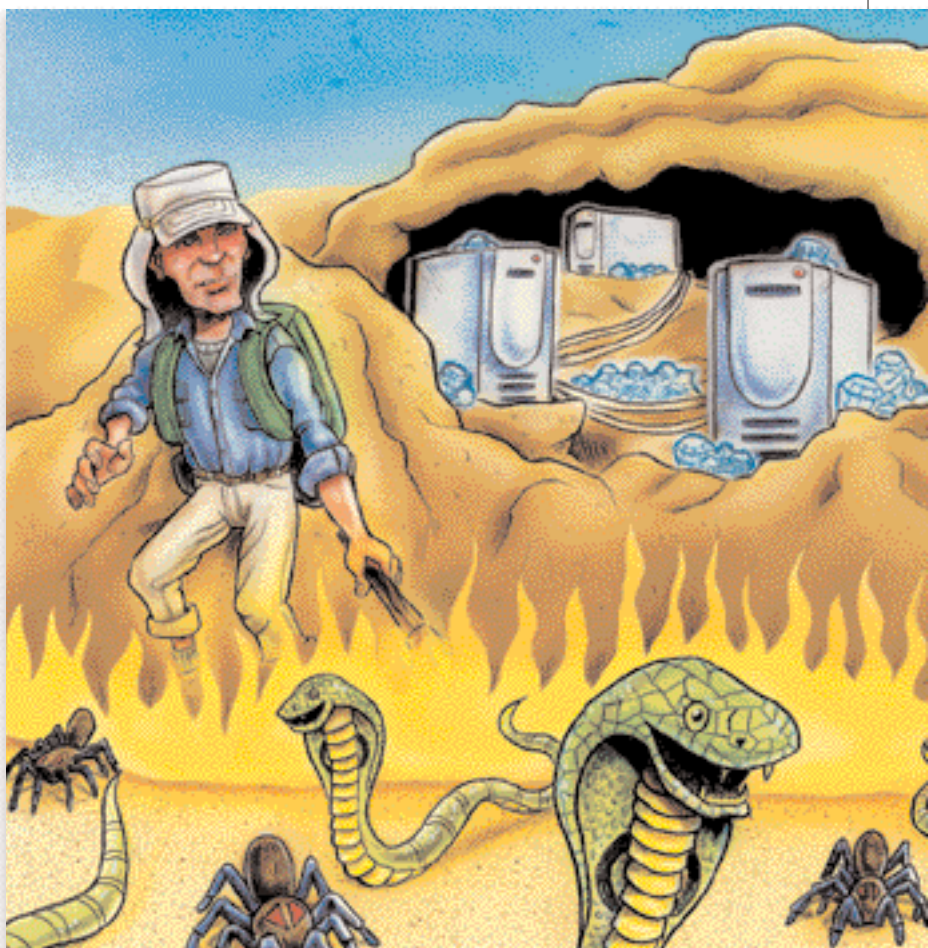
**Consider stalled IT budgets and a lingering feeling of insecurity a mandate to get a handle on new security technologies and products in 2003.** Of course, with vendors bombarding you with an ever-widening range of gee-whiz security gizmos, that's easier said than done.

The first step: Identify what you need to protect, from physical assets to digital data. Then consider how your applications function, what access these applications and your users need, and who will be using the information.

You're probably thinking, "Easy for you to say." Out there in the trenches, after you finish configuring your firewall, deploying your VPN, monitoring your IDS, updating your virus scanners, examining your logs, getting current on the latest vulnerabilities, keeping up with the endless stream of patches and putting out fires, there's precious little time to fine tune your security architecture.

The solution: Know when to delegate. Many day-to-day tasks can be outsourced to an MSSP (managed security service provider), provided you do your homework and ensure the MSSP can offer 24x7 management and monitoring. Installing and configuring firewalls and deploying VPNs, for example, are prime candidates for outsourcing. As long as you have a view into the provider's configuration to ensure changes are made properly, you can safely shed some of your workload.

By outsourcing you'll not only free up time to focus



on more important security issues, you'll gain additional benefits. Unless you're Superman, you can't do it all, nor can you be an expert in everything. Reputable outsourcing firms that focus on security can bring to bear some of the best talent and technology in the industry. Furthermore, multinational MSSPs, such as Symantec Real Time Managed Security Services (formerly Riptech) and Internet Security Systems, can detect new attacks early because of their broad view of traffic.

Although technology advances are valuable, without a road map you'll be deploying security products higgledy-piggledy. Security documents, like standards and

## SECURITY

acceptable-use policies, serve several functions critical to the management of your business. We know many of you have developed security policies *and* we know many of those security policies are gathering dust. And while there has been an increase in spending, the percentage of security dollars in most IT budgets remains relatively small, largely because security is seen as a cost. To argue for an increase in your budget, you must make it known that security functions support the business plan. That means keeping your security policy current and showing how it will support all other facets of your company's strategy.

### Take a Risk

A key driver for increased security spending is risk management, which tries to mitigate overall risk, defined as "the probability that an organization will lose assets during a successful attack." Risk management entails a few tasks: First, determine the criticality of your assets. If a system is unavailable or if data is stolen, what will be the

overall impact to the organization? Next, perform a risk assessment, examining your systems and operation policies to determine the likelihood of a successful attack. Then, define policies, implement procedures and deploy products to mitigate the risks you've discovered. By showing how you can protect business assets from loss, and what the potential loss could be, you will have a justification for increasing security spending.

Furthermore, your security policy may be used by external auditors to ensure that your business processes are run in a secure manner. Just like a financial audit examines profit, loss and the accounting methods used to calculate profit and loss, a security policy tells auditors what processes are in place and how your organization protects information assets. Regulations such as GLBA and HIPAA have privacy and protection requirements.

### Living Dangerously

Several key security areas will deserve your attention in 2003. While it is fun (for some of us, anyway) to theorize

## Companies To Watch

#### ARCSIGHT

ArcSight is making strong moves into the SIM space, a product area we see as key for enterprise security management.

#### INTRUVERT NETWORKS

IntruVert's thing is high-speed IDS—up to 2 Gbps—and enterprise management. And its IntruShield is OSEC-compliant to boot.

#### NETSCREEN TECHNOLOGIES

NetScreen makes the definitive hardware firewall. With its recent acquisition of OneSecure, the company is poised for some interesting integration between the product lines.

#### NORMAN DATA DEFENSE SYSTEMS

Just when you thought you knew virus detection, Norman Data Systems is putting a virtual PC in its engine to actively monitor application activity. Suspicious code is identified by what it does, not by how it looks.

#### NOVELL

Novell's strength is in eDirectory, NMAS and iChain for authentication, user management and access control. Now if the company could only get the marketing right.

#### OKENA

Okena's StormFront and StormWatch products are leading the HIP space, and we expect to see improvements in the coming year.

#### SILENTRUNNER

SilentRunner, a subsidiary of Raytheon, is repositioning its network intrusion detection product as a network forensics and monitoring tool.

#### SYMANTEC

With its recent acquisitions of Recourse Technologies and RipTech and its previous purchase of Axent, Symantec is making a strong play into the enterprise market.

#### TIPPINGPOINT TECHNOLOGIES

TippingPoint is addressing the need for high-speed IDS with more intelligent event reporting. Although we had some problems in initial tests (see "Tipping the Scales," [www.nwc.com/1320/1320sp1.html](http://www.nwc.com/1320/1320sp1.html)), the company is on the right track.

#### ZONELABS

Known for its personal firewall, ZoneLabs is making a huge play for centrally managed desktop firewalls through a strong management platform and an aggressive partnering strategy.

## SECURITY

about possible attack vectors, in reality, you need to worry about only a handful. These include mobile code, poor application programming, faulty network design and remote device vulnerabilities. Following are the biggest dangers and the most practical advances for combatting them.

**DANGER: MALICIOUS MOBILE CODE AND EXECUTABLES****SOLUTION: USE SANDBOXING**

Forty-four percent of respondents to Information Week's 2002 Global Information Security Survey ([www.informationweek.com/story/IWK20021003S0011](http://www.informationweek.com/story/IWK20021003S0011)) reported attacks stemming from viruses, worms and Trojans, down from 70 percent year over year. The drop could be due to less malicious code in the wild or increased deployment of antivirus software after Nimda or Code Red, or both. Although antivirus software is decidedly reactive, vendors

## Given enough experience and knowledge, an admin can make sense of the data and perform some real investigative work.

have shortened turnaround times to several hours after a breakout, so antivirus engines are updated in a more timely fashion.

The holy grail, of course, is squashing an unknown virus before it activates. But this is tricky because there are few, if any, reliable detection engines for new forms of malware. This is where virtual computing may be just the ticket, and Norman Data Defense Systems is leading the way. The idea is to run downloaded content and watch for virus- or wormlike behavior, such as binding to network ports or accessing mail resources via MAPI. By running the code inside a virtual computer, run-time actions

can be monitored and malicious activity identified. Of course, there are limits to the virtual PC. Simulating an operating system is relatively easy; simulating an operating system and an office application suite is not.

**DANGER: THE PERIMETER IS EXPANDING****SOLUTION: ENFORCE POLICY ON REMOTE SYSTEMS**

If remote users are attaching to the network over dial-up, VPN or wireless PDA, your perimeter is in constant flux. And though you can secure the endpoints and the traffic flowing between them using antivirus software, desktop firewalls, VPN software and SSL, having all these technologies deployed increases the burden of managing, maintaining and logging those remote applications.

By using security products on remote computers, you enforce your policy uniformly. Before you let users connect, make sure their antivirus signatures and firewall policies are up-to-date, allow only the access you permit, ensure their operating system and applications are at the proper patch levels, and check that unapproved services are not running. Desktop security packages offer varying capabilities to enforce a baseline of acceptable computer configurations and are improving over previous versions. Features—such as version control for executables and dynamically linked libraries, file hashing and validation, requiring that applications are current and active prior to a connection, and error messages telling users when their computers don't meet the requisite specs and how to fix them—should be atop your list of requirements.

This protection should be deployed within the internal network as well. Every entry point into your network is a possible avenue of attack, and your most successful strategy is to put controls closest to the threat.

**DANGER: ATTACKERS TARGETING YOUR APPLICATIONS****SOLUTION: GET HIP TO INTRUSION PREVENTION**

Intrusion prevention is all the rage. The theory is, if you block attacks before they reach their targets, you're gold-

## Standards

**CISSP**

Not really a standard, but an industrywide certification that indicates the bearer has in-depth knowledge of multiple security principles. See [www.isc2.org/cgi/content.cgi?category=19](http://www.isc2.org/cgi/content.cgi?category=19)

**COMMON CRITERIA**

Common Criteria provides certification for specifically named and configured systems and subsystems against a given set of requirements. The value is not necessarily in the certification, but in the public technical documents detailing the product's design and testing. See [www.commoncriteria.org/docs/aboutus.html](http://www.commoncriteria.org/docs/aboutus.html)

**ISO 17799**

An international standard that describes and details policies and procedures ranging from business continuity to physical and network security and security policies. See [csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf](http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf)

**SAML**

Security Association Markup Language is an XML-based standard that lets Web services exchange authentication and access control data seamlessly. Version 1.0 was approved by OASIS on Nov. 6. See [www.oasis-open.org/committees/security/](http://www.oasis-open.org/committees/security/)

## SECURITY

en. But the question is, can intrusion prevention deliver?

NIP (network intrusion prevention) products monitor traffic at key network points and attempt to block attacks dynamically while allowing legitimate traffic. Don't believe the hype. Unfortunately, these products rely on the imperfect detection methods used in NIDS (network intrusion detection systems), such as signature matching and anomalous traffic detection. Although many well-known attack signatures exist, new attacks using unknown methods are bound to rear their ugly heads. In addition, legitimate traffic may be blocked because of poorly written attack signatures flagging normal traffic as malicious.

HIP (host intrusion prevention), on the other hand, offers greater promise for blocking known and unknown attacks at the target. HIP enforces access control to the operating system and system services. By defining what an application can or cannot access, all manner of attacks that leverage operating system services can be thwarted because attackers exploit vulnerabilities that provide access outside the application's normal operating parameters. System calls trapped at the kernel level are matched to policy and, if denied, are stopped. Pure application-layer attacks, such as those that attempt to manipulate database tables and data but don't request system services, are not deterred by HIP, however, and developing and deploying HIP policies can be complicated and time-consuming. But given the increased protection, that's a relatively small price to pay. We expect HIP applications to become more robust and manageable over the next year as Okena, Computer Associates, Harris, Enterscept and other vendors modify their protection applications based on user feedback and deployment experience.

#### **DANGER: A DELUGE OF EVENT DATA SOLUTION: RELY ON SIM**

Once your network security has gotten to a point where enough components, such as firewalls, IDSs and VPN gateways, are deployed or outsourced, you can spend time monitoring logs and mentally correlating events. Given enough experience and knowledge of individual systems, a seasoned administrator can make sense of the data and perform some real investigative work. Unfortunately, getting to that point is difficult and, let's face it, manually correlating data is time-consuming.

That's where SIM (security information management) data aggregation and correlation tools come in. Event aggregation is simple compared with event correlation because there are few formalized methods for accurately correlating disparate events into a single, related chain. But don't overlook the difficulties tied to event aggregation. As the number of devices feeding events into the SIM product increases, so do storage, bandwidth and horsepower requirements. And getting all these products to talk to each other is, well, daunting. The value of SIM diminishes if you can't get all your data sucked in.

Let's say you have data aggregated. Now you can

begin to mine it for relevant events. That's the point of SIM, right? Separating the wheat from the chaff? Although there are some common event sets that can be applied to most networks, you can bet you'll be doing (or having done for you) a lot of customization. This is not a fire-and-forget technology by any means.

Is there a benefit to SIM? Sure. If your security administrators can work more efficiently and effectively, that's a big win for already overworked staff. But you have to determine whether the costs will justify the gains. **NWC**

*Mike Fratto is a senior technology editor based in NETWORK COMPUTING's Syracuse University Real-World Labs®; he covers all security-related topics. Prior to joining this magazine, Mike worked as an independent consultant in central New York. Write to him at mfratto@nwc.com.*

## WebLinks

- » "Security Fears Are Up, So Why Is Spending Down?" (TechWeb, Nov. 2, 2002) [www.techweb.com/tech/security/20021106\\_security](http://www.techweb.com/tech/security/20021106_security)
- » "The Rules of Electronic Record-Keeping" (NETWORK COMPUTING, Nov. 1, 2002) [www.nwc.com/1323/1323ws1.html](http://www.nwc.com/1323/1323ws1.html)
- » "Keep Out" (NETWORK COMPUTING, Oct. 21, 2002) [www.nwc.com/1322/1322f1.html](http://www.nwc.com/1322/1322f1.html)
- » "Add Some Fiberlink to Your VPN Diet" (NETWORK COMPUTING, Aug. 19, 2002) [www.nwc.com/1317/1317f3.html](http://www.nwc.com/1317/1317f3.html)
- » "InfoExpress CyberGatekeeper Ensures Remote Users Comply With Security Policies" (NETWORK COMPUTING, May 13, 2002) [www.nwc.com/1310/1310sp3.html](http://www.nwc.com/1310/1310sp3.html)
- » "Track Service-Desk Activities Using UniPress FootPrints 5.5" (NETWORK COMPUTING, May 13, 2002) [www.nwc.com/1310/1310sp4.html](http://www.nwc.com/1310/1310sp4.html)
- » "Desperately Seeking the Security ROI" (NETWORK COMPUTING, May 22, 2002) [www.nwc.com/1311/1311colshipleigh.html](http://www.nwc.com/1311/1311colshipleigh.html)
- » "Security Information Management Tools: NetForensics Leads a Weary Fleet" (NETWORK COMPUTING, April 2, 2002) [www.nwc.com/1307/1307f2.html](http://www.nwc.com/1307/1307f2.html)
- » "Bear Stearns Adds an Extra Layer of PC Protection" (NETWORK COMPUTING, Feb. 18, 2002) [www.nwc.com/1304/1304centerfoldtext.html](http://www.nwc.com/1304/1304centerfoldtext.html)
- » "Risk Management" (NETWORK COMPUTING Tech Library) [techlibrary.networkcomputing.com/data/rlist?t=itmgmt\\_10\\_50](http://techlibrary.networkcomputing.com/data/rlist?t=itmgmt_10_50)
- » "IT Reaches for Help" (InternetWeek, Aug. 28, 2001) [www.internetweek.com/indepth01/indepth082801.htm](http://www.internetweek.com/indepth01/indepth082801.htm)
- » RFP/RFQ Builder [www.nwc.com/go/sec-rfp.html](http://www.nwc.com/go/sec-rfp.html)
- » White Papers [www.nwc.com/go/sec-papers.html](http://www.nwc.com/go/sec-papers.html)
- » Research Reports [www.nwc.com/go/sec-res.htm](http://www.nwc.com/go/sec-res.htm)
- » Careers [www.nwc.com/go/sec-jobs.htm](http://www.nwc.com/go/sec-jobs.htm)
- » Books [www.nwc.com/go/sec-books.html](http://www.nwc.com/go/sec-books.html)
- » Training [www.nwc.com/go/sec-train.html](http://www.nwc.com/go/sec-train.html)
- » Forum [www.nwc.com/go/shoptalk.html](http://www.nwc.com/go/shoptalk.html)
- » Newsletter [www.nwc.com/go/sac.html](http://www.nwc.com/go/sac.html)