SLAYING THE 'NET DRAGONS

by Judith Harper

In the ancient world, map-makers carefully marked uncharted regions to warn unsuspecting travelers: Here Be Dragons. Early-adopting IS managers steering their organizations through Internet/intranet/extranet seas typically had few maps and even fewer posted warnings. The pioneers quickly found out that 'Net dragons do exist. They're real, they're quick, and they're mean.

"Without secure Internet connectivity, you open yourself to tremendous misuse both inside and outside the organization," says MacDonnell Ulsch, managing partner at the National Security Institute (Westborough, MA). "The absence of security creates risk that can kill your business."

Out there--in the uncharted waters of the Internet --be Hackers. And Hacked-Off Former Customers. Or Hacked-Off Former Employees. Or Competitors. Or Low-Down Dirty Thieves. Or "a whole new group of people I call cyber-vandals" says Rob Clyde, a vice president at AXENT Technologies. "Their interest seems to be in destruction. The old hacker 'ethic' was about proving that you could break in and then bragging about it afterwards. This new breed just wants to wreck things." Indeed. The ‘Net can be a Very Scary Place.

Even worse, dragons in employee's clothing can make the unsecured intranet an equally Scary Place. "The FBI estimates that 80% of all network attacks are internal," says Christopher Klaus, founder and chief technology officer for Atlanta-based Internet Security Systems (ISS). "Many people use our products to monitor employees and make sure they're not e-mailing sensitive data from one department to another."

'Net pioneers may have been taken unawares, but today's managers have read the warning signs. "Those still believing there is no problem are in the vast minority," says Clyde. "Over 60% of published survey respondents report that their networks are penetrated more than 30 times a year. Our Infosecurity SWAT Team has found 10,000 hacker sites on the Web, all providing instructions about how to break into systems."

How Much Security Is Enough?

The threat is real. Sensitive files may be intercepted and read, edited, or misdirected. Anonymous mischief-makers may use your identity to send spurious e-mail in your name. System files may disappear, servers may crash, and strangers may divert funds, compromise trade secrets, or harass customers and employees electronically.

The potential for loss is enormous. More than half the Fortune 1000 firms polled in a 1996 survey (conducted by Baltimore-based WarRoom Research LLC) reported losses greater than $200,000 for each successful intrusion into their computer systems. For better than 15% of the respondents, the loss per incident was more than $1,000,000.

What can you do about it? What is good security? How much security is enough? What steps do you take to implement it? Those answers are never exactly the same for any two organizations. Your security implementation must fit into the overall corporate strategy, which is different for every company.

"Good security is balancing the cost of the security measures you put in place with the level of exposure you're willing to accept," says Clyde.

No system is completely protected; the laws of Nature and of Murphy guarantee that security will be breached by somebody or something sooner or later. *Absolutely no unauthorized access* sounds great as a goal, but can you really get there? Practically speaking, the secure system makes the breach later rather than sooner, smaller rather than catastrophic, and quickly detectable rather than unnoticed.

Many managers make decisions based only on what they read in the press, says Ulsch. "Security is important. Fireballs are hot. Intrusion detection is hot. They don't understand that security is an ongoing management process."

Moving toward Security

As with any management process, effective security begins at the top. In many companies, the responsible executive would be a Chief Information Officer (CIO). "Whether it's the CIO, the CEO, or the COO," says Ulsch, "someone in senior management needs to say, 'Security begins and ends with me, and we will take it seriously.'"

"A fundamental problem with network security today is that senior management is not entirely certain that good, robust security is a vital part of the IT infrastructure. But we know that it is. Any organization that does not subscribe to that fact is increasing its level of risk to serious intrusion and even liability."

Without high-level support, security issues and personnel become merely defensive and reactive, rather than proactive. A champion at the senior- executive level puts security on the radar screen for the organization. "The difference is that people in senior management can understand the criticality of security and appreciate the fact that it is an enabling technology to help generate revenue via electronic commerce," says Ulsch. "That's a key issue."

Ulsch recommends integrating physical plant security and network security. The former is "more than keeping people from carrying computers out through the front door," and the latter is "more than monitoring the firewall. Migration to the next level integrates both functions under a chief security officer charged with responsibility for total enterprisewide security."

Establishing the Policies

"The balance point – where the cost of security measures is inline with the level of exposure you're willing to accept – is the critical point, the sweet spot for security," says Clyde. "A good security policy hits that sweet spot."

Security policies specify standards, guidelines, and procedures; they spell out what it means to protect your

information systems. Most companies have security policies; most security policies, however, do not hit the sweet spot. "We see people who don't even think about their security policies, much less enforce them, until they're successfully attacked," says Klaus.

"The key (to developing workable policies) is to look at a best-practices approach," says Clyde. "Don't start in a vacuum." When developing and/or refining your security policies, ask some basic questions:

1) What assets must be protected? Where are they? What are they worth?

2) How are the assets threatened? What are the dangers?

3) Where are the points of vulnerability? Are they widespread or concentrated? Are they internal or external?

4) How great are the risks? Can the risks be quantified?

5) What steps can I take to minimize the risks?

"Make sure you have certain policies in place," says Sam Glesner, field support manager for International Computer Security Association (ICSA, based in Carlisle, PA). "Some of the things we look for are:

- A privacy policy for Web clients

- A network access policy for system users (who has access, how access is controlled)

- An Internet security policy (who can access the 'Net from your system, what should/shouldn't be encrypted, what is confidential, what is not)

- An Internet application development policy (procedures or posting Web content, what programs used to maintain the site and make it accessible)

- Physical security policy (who is allowed in, what about visitors, emergency contacts)"

Security product and service vendors are always ready to offer assistance, but be wary. "When you're selling hammers, every problem looks like a nail," says Ulsch. "Look for a vendor who understands security, who will look inside your organization and develop a security strategy that fits your situation and your corporate strategy. Interview several; find out what they know." It's important to maintain a high level of vendor-independence.

Sweat the Small Stuff

Before you look at the technical details of securing the bits and bytes of network connections, system security and protection against outside intruders, make sure the basics are under control. Here's a basic security/housekeeping checklist that covers some of the small stuff.

Personnel-- Is a clear security policy in place? Do employees wear ID badges? Have all employees undergone awareness training? Are regular security audits held?

Physical Security-- Are wiring closets locked? Does staff challenge strangers? Are unattended workstations left online? Are keyboards locked when unattended?

Authentication-- Are passwords required to be changed periodically? Are there standards (length, mixed case, etc.) for passwords? Are there strict requirements for authorizing new users? Are old/terminated/unused accounts completely closed out?

Disaster Recovery-- Is there a standard, required backup procedure? Are backup media stored in safe place (preferably off-site)? Are backup media verified on a regular basis? Are backups encrypted?

Assessing the Risk

"You need to continually challenge the security you have in place," says Ulsch. "That can be done by having internal teams or trusted third-party service organizations constantly attack your network to find vulnerabilities."

Companies like ICSA will "walk up to your network door and see if it is unlocked. If it is, we let you know," says Glesner. "We run a test suite against someone's IP addresses to see what services are visible to the Internet. Then we can give them feedback on how to make themselves more secure."

A common-sense approach to controlling your vulnerability means accessing current, state-of-the-hack information:

- Know what holes have been found in your operating system. Install the vendor's latest patches.

- Be alert for signs of intruders. Check the status of your system files to ferret out Trojan horses just waiting for an opportunity to go to work.

- Make sure your applications are set up for auditing.