# Best Practices in Network Security

March 20, 2000

Frederick M. Avolio

Information systems security. Computer and network security. Internet security. It's a complex world, and growing more so every day. With these changes, some truths and approaches to security remain the same, while others are new and radically different. Developing a sound security strategy involves keeping one eye on the reality of Internet-speed changes in threats and technology, and the other on the reality of the corporate environment. Purchasing security devices is easy. Knowing how and what to protect and what controls to put in place is a bit more difficult. It takes security management, including planning, policy development and the design of procedures.

**Not Your Father's Network**

When the computer and network space was simpler, you could expect a network to support any IP service. However, most people stuck to the basics of terminal service, file copying and e-mail, with some file sharing thrown in. Fewer services meant fewer avenues of attack.

Today's network incorporates all sorts of wonderful but unsettling services. Voice data travels over the enterprise network. Files are shared. Corporate networks now include travelers and customers, often in the name of e-business and e-commerce. Every new network service represents possibilities for increased sales.

Businesses reach out and touch partners, customers and potential clients, often via the Internet. According to the January 2000 Internet Software Consortium's Inter- net Domain Survey (www. isc.org/ds), there are more than 72 million hosts on the Internet. Given that many organizations do not advertise their internal name spaces, we know that many more computers are connected in some fashion to the Internet. Potentially, perhaps a billion people live in the "network neighborhood."

Between the vastness of this space and the services available, there are countless potential avenues of attack. Attackers don't even have to be particularly smart, skilled or patient to develop an attack. Through the ease of "user friendly" software, and with the ubiquity of methods for simple file distribution, anyone with a computer is a potential at- tacker. No special skills are required. Launching attacks is within the reach of anyone with a mouse.

## The New Ground Rules

To meet the challenges of computer and network security, it's crucial to adopt ground rules. Once they're in hand, the rest is easy.

1. Security and complexity are often inversely proportional. Every step taken--whether it's vulnerability and risk assessment, security policy and procedure development, deployment of mechanisms or user education--should be as straightforward and simple as possible. The more cryptic the instructions and procedures, the more room for misunderstanding and misapplication.

2. Security and usability are often inversely proportional. There is no such thing as "complete security" in a usable system. Consequently, it's important to concentrate on reducing risk, but not waste resources trying to eliminate it completely. Such a pragmatic mind-set provides a fighting chance to achieve fairly good security while still allowing productivity.

3. Good security now is better than perfect security never. This is a corollary of the previous axiom, since perfect security doesn't exist in a usable system. Even if it were possible, a usable system is a moving target: Threats change, technologies change and business needs change. The job is never done.

This knowledge should actually free you to shoot for "good enough." Come up with 10 things to do, but only get to four of them now, and you're probably in a better position than if you wait until it's possible to do all 10. The key is to prioritize correctly.

4. A false sense of security is worse than a true sense of insecurity. Knowing where your enterprise is still insecure provides you with the framework for moving ahead. It's critical to know where you've left gaps, what documents and procedures are not quite right and what mechanisms need replacing. A false sense of security does not motivate improvement--or even analysis--of an organization's security posture. It leads to false complacency, which can give rise to disaster, often accompanied by the lament, "I thought we had that covered." It's better to know where you are weak and avoid unquantifiable risks.

5. Your security is only as strong as your weakest link. Therefore, be thorough in examinations and evaluations. For example, if there's a reason to employ VPNs (virtual private networks) to keep connections from home and remote offices to headquarters private, it may be necessary to protect that data while it resides on the notebook PCs of your mobile workforce. It may mean removing modems from desktop computers, requiring all traffic to flow through the firewall.

6. It is best to concentrate on known, probable threats. There are imagined threats, real threats and probable threats. And there are known and unknown threats. We are most interested in real and probable threats, while we continue to expand the set of known threats.

7. Security is an investment, not an expense. The challenge is to get this point across to upper management. Investing in computer and network security measures that meet changing business requirements and risks makes it possible to satisfy changing business requirements without hurting the business' viability. Properly secured servers let corporate information be shared with salespeople in the field and with business partners. Improperly configured systems lead to data loss or worse.

Although it's comforting when an attack is put off, it is much better never to have to put security measures to an actual "battlefield" test. As with airbags in an automobile, it's important that they're there, but better never to have to use them. With these ground rules in mind, it's time to do the most important work in securing networks and computers: security management. Keeping the above axioms in mind should help you streamline the process.

**Planning: The Team Determines the Needs**

The security planning team should include people involved in different aspects of IT from different areas of the enterprise. Creating the policy will be a group effort, and responsible representatives from different departments should be involved to keep communication flowing. Knowledgeable people, savvy in business requirements, technology and security, are necessary. Few will be up to speed in all these areas, which is one reason for the group effort. IT staff members--systems and network administrators--must be involved.

Once the team is created, the first step is an analysis of business requirements. What services are required for business, and how might those requirements be met securely? The hardest part is distinguishing wants from needs.

The team, with all its members' viewpoints, determines the business needs for computer and network services. How much do employees depend on Internet access, use of e-mail and availability of intranet services? Drill deeper and look at particular computer and network services. Do they rely on remote access to the internal network? Is there a requirement for access to the Web? Do customers access technical support data via the Internet?

For every service, it takes discipline to ask repeatedly, "Is there a business requirement?" But that's the most important question.

**Threats, Vulnerabilities and Risks**

The planning phase involves development of what can be called vulnerability analysis, risk analysis or threat assessment. Although the terms have slightly different definitions, the end results are similar. This phase encompasses asset identification and evaluation; postulation and analysis of threats; vulnerability assessment; appraisal of existing countermeasures, and cost/benefit analysis. Numerous factors are considered, including how information is used and managed, and how good and relevant existing security measures are. Assets (including information) as well as threats are classified. The goal is to consider the things indicated as business requirements.

This is another reason to create the team of people from different areas of the company. While some of the team members' opinions may be off-base, the cross-section of disciplines provides a more complete picture than one gotten by interviewing people in marketing, sales or development. This is the time to ask questions such as these:

- What are we trying to protect? Corporate image? Future product plans? Employees from recruiters? Personal information? Client information? Computer resources? All are possible and all could be valid.

- Which attacks are possible? Which are probable?
- Where are we vulnerable? Vulnerability-assessment tools can help pinpoint those areas (see "Resources," page 68). Don't forget to consider people as a source of vulnerability. Employees who answer telephones, business partners with access to proprietary information, and customers who access the support database all are potential threats.
- What are we concerned about keeping? What would we hate to lose? What are these items worth? How much would it cost to replace them? What would it cost to lose them? (Another benefit of a group: Some will see the material costs while others will think of intangibles, such as costs to reputation and investor confidence. Both opinions are useful.)
- How valuable would the following be to an attacker (possibly a competitor): our company losing data, our hurt reputation or a competitor acquiring data?
- How much would it cost an attacker to attack us?
- How much would it cost to counter?
- What security measures are in place? Are they working? Are they relevant?

It's possible to classify threats on a scale of 1 to 5, or to put them into categories, such as: "Fix immediately," "Uncertain--needs more study," "Watch closely, but don't take immediate action," "Don't care." In this way threats are classified, vulnerabilities are assessed and residual risks are cataloged.

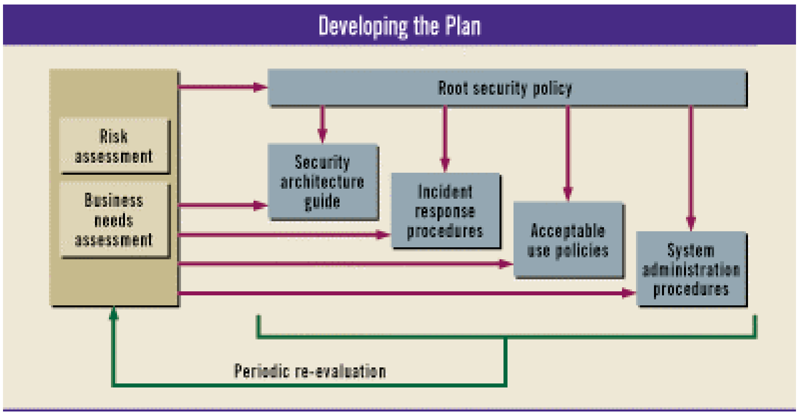
**Root Security Policy**

With this preliminary work done, it's time to develop the root security policy. This is where the risk assessment and business requirements come together and where differences are worked out. The root security policy addresses how an organization handles information, who may access it and how. It also specifies allowed and denied behavior. And it lists controls that are in place.

This high-level document provides the framework upon which all required information and subpolicies hang. The root policy's top-down approach makes it possible to adhere to the guidelines and produce meaningful and useful work, without the pressure of having to get it 100 percent correct and complete from the start. This framework lets anyone look at the document anytime, and see where the holes are. There are resources on the Internet and in books to assist in this step. There are even samples of policies and related documents.

The root security policy typically includes the following items:

- Root security policy overview
- Security architecture guide
- Incident-response procedures
- Acceptable use policies
- System admin procedures
- Other management procedures


Developing the Plan
Root security policy
Risk assessment
Business needs assessment
Security architecture guide
Incident response procedures
Acceptable use policies
System administration procedures
Periodic re-evaluation

There is no magic here. You may have more sections. You may have fewer (see "Developing the Plan," above).

The overview explains the purpose of the policy document, describes its makeup, details who is responsible for what and states the procedures and expected time frames for making changes. Remember, the ground rules say some things are bound to go wrong, and requirements and threats will change over time. Stating up front how to get things changed helps people more easily accept the policy and related documents. Doing so also calms the concerns of policy-shy management.

### Security Architecture Guidelines

The security architecture guidelines specify countermeasures to the threats discovered in the risk assessment. This document dictates, for example, where to place firewalls, when to use encryption, where to place Web servers and how to allow communication with business partners and customers. It may identify particular products and give instruction on how to deploy and manage them. The security architecture guidelines specify the assurances that are in place, the auditing and the controls.

This part requires expertise, which you may acquire through the services of an outside consultant or in-house through education, including Web-based resources, books, technical papers and conferences. Among other sources, The SANS Institute (www.sans.org), The Internet Security Conference (tisc.corecom.com) and Computer Security Institute (www.gocsi.com) provide training.

### Incident Response Procedure

One of the management procedures in the root security policy is the incident response procedure. What is considered an "incident" in the first place? What happens when a security incident is discovered? What is done when the attacker calls? Who gets called and when?

It's useful to test the procedure with a sort of incident-response procedure drill. People to consider calling may include officers of the company, the marketing manager (for press relations), system and network administrative staff, and the police. When you call them, and in what order, must be part of the procedure. Calling too many people too soon risks letting the cat out of the bag, so to speak, or a crying wolf scenario. Calling too few people, too late, risks lawsuits.

Although this process does not require any particular technical expertise, it does require a lot of thought. Senior managers should carefully review this document, after receiving a briefing based on the vulnerability assessment. The goal is to scare them, but not too much.

### Acceptable Use Policies

The root computer and network security policy will point to various acceptable use policies. (Some call them acceptable use guides, but that makes them sound negotiable.) The number and type of policies depend on the analysis of your business requirements, risk assessment and corporate culture. The acceptable use policies are meant for end users. They explain which actions are permitted and which are prohibited. So there may be acceptable use policies for computers, transfer of data, e-mail communications, notebook PCs and Web access.

Recall that these documents are part of (really, hung on the framework of) the root security policy. You will not sit down one day and write five or 10 acceptable use policies. Rather, you'll put entries--"To Be Written" --into the root policy to act as placeholders. As your committee assigns writers, you'll enter their names next to the notation, and after they write it, the root policy contains it or, more usually, points to it.

There is no special format for an acceptable use policy. It should name the service, system or subsystem it is regulating (for example, computer use, internal and Internet e-mail, notebook computers and password policy), and state in the clearest terms behavior that is and is not permitted. The policy should detail the consequences of breaking the rules.

### System Policies and System Administration Procedures

With a proper understanding of the business requirements and the risks, and with the security architecture guide in place, your organization can develop platform-specific policies and related procedures. These often lead to lock-down guides that address organization-specific steps for hardening vendor-supplied systems. Lock-down guides are usually products of the system administration staff, with information gleaned from experience, books and reference guides. Also, specified here is what software must and must not be in place, and how the systems are to be backed up and administered.

### Other Management Procedures

Management procedures also spell out how information is marked and handled, and how people can access that information. They establish a principle of "need to know" and attempt to match access with need.

### Management Buy-In

Unfortunately, if senior management is not committed to information security, your best efforts are wasted. Senior management has to see the inseparable link between computer and network use and computer and network security. Just as it (probably) sees computer, network and telephone costs are part of the investment for doing business, so must it see security costs. Tying security and services together gives an honest picture of the cost while linking the cost of security with the benefits of the service. Security costs can then be seen as a profit enabler.

Someone from senior management should be involved in the process. Although a corporate security officer is probably too much to ask for, you should be able to settle for an information systems security manager who reports to senior management. This manager should have the responsibilities and corresponding authority for the job. This also signals to the organization the importance of good security practices.

Senior management must ratify every policy, document or guideline. This does not mean having the board of directors approve every change to every plan. Rather, it means the senior staff is aware of the work being done, and supports it by affirming changes. Security policies alone have no teeth. Corporate management support supplies that. If senior management does not support parts of the work, they are essentially dead.

Overwhelmed? Remember, this can't all be done at once. You will leave things out and get things wrong. Address the known requirements and threats. This is one of the benefits of a root policy as a framework. It tells us what has to be done. Do what's possible today, tag residual risks and note tasks to be accomplished. Will you get perfect security? No. Rather, you'll achieve timely, usable and sufficient security in the midst of an increasingly dangerous, but exciting networked world.

# Is Security the Next Big Thing?

When it comes to enterprise network security, our survey respondents seem to be a very confident bunch. Are they just deluding themselves? By Greg Shipley

**Corporate security is an** extremely slippery topic. People love to talk about it, but few seem to get their hands around it. Therefore, we shouldn't have been surprised when we inquired about the state of information security and received feedback from more than 500 organizations.

More than 80 percent of our respondents said they determine the need for, evaluate and specify which security products to purchase--so we definitely heard from those in the trenches. Nearly 90 percent have implemented firewalls and virus-protection software, and more than 60 percent think their security policies are both relevant and up-to-date. What's the No. 1 security-related product people are looking to add in the next 12 months? More than 42 percent cited intrusion-detection systems. Most claim they have the basics down and are moving to more complex protective measures.

Finally, when we asked organizations about their overall attitude toward their information security policies, only 15 percent responded that they wished they still had their "blankies." This could be a good sign, as people are confident in their security endeavors--or at least they no longer covet soft, inanimate objects.

Organizations claim to be on top of their security policies, are spending money on security and security products, and say this spending will increase over the next few years. So we've got to ask, What's the problem? Why are corporations worldwide continuously getting pummeled? Heck, if RSA Security can't keep its Web site from getting hacked (see www.attrition.org/mirror/attrition/2000/02/12/www.rsa.com/), how can the rest of us be so confident? (OK, so RSA's DNS got hacked and people went to the hacked site instead of the real one--but the result is the same.)

Although we can draw some interesting conclusions from our survey, our observations have less to do with trends and more to do with a larger problem. Companies are starting to take security seriously--a good thing--but perceptions are still in dire need of adjustment. It's almost as if the industry is in denial: "We've got our security down...or we think we do, anyway." For example, we found it particularly curious that while more than 60 percent of all respondents think their security policies are up-to-date, only 23 percent of them review their policies at any reasonable level of frequency--i.e., weekly or monthly. Another trend that doesn't quite match up is the apparent desire to outsource. If confidence is so high, why are more than 54 percent of the organizations outsourcing their firewall management, and 34 percent outsourcing their virus-protection efforts? Perhaps confidence is so high because there is someone else to blame. On the staffing front, 63 percent of the respondents claim they have no dedicated IT security staff. Either our respondents employ some of the most security-conscious administrators around or their strategies have some serious holes. It just doesn't add up.

So it appears that we can look forward to a definite interest in security, and increased product sales. It appears that intrusion detection will be a hot item this year. And it appears that many organizations are confident in their approaches to information security. Yet as computer crime statistics skyrocket, we are led to believe otherwise. Or maybe we're just too darn cynical. Maybe the fact that organizations don't have full-time security staff just means they've taken security to the next level and have integrated it into their business processes. After all, who filled out this survey? Network Computing readers--that's who. And we all know that group is already ahead of the pack. For the complete results of our survey, see img.cmpnet.com/nc/1105/graphics/f22.pdf.

# Executive Summary

**Best Practices in Network Security**

One of the side benefits of the Internet's growth, with the accompanying reports of computer and network break-ins and computer virus infections, is the increased awareness and acceptance of computer and network security policies, procedures and mechanisms. As our use of computers and networks expands, so does the list of things that can go wrong and ways our organizations can be hurt.

Security policy, procedure and proper-use documents give system and network administrators something to fall back on in a crisis, as well as guidance for the mundane but essential day-to-day decisions and actions. They also provide approaches to problems that have been well-thought-out and tested over time. And though there is no magic in them, these policies bring an organization closer to understanding its computer and network business requirements and risks. At the same time, the policies provide a framework for re-evaluation as requirements and risks change.

The work of instituting the best practices for network security can be daunting. The list of tasks seems limitless, and the possible procedural issues appear to touch on every aspect of every employee's interaction with the network.

The correct framework built on the correct premises makes this easier to accomplish. Premises firmly grounded in reality, that take into account the needs for both usability and security, give us the freedom to thoughtfully and calmly provide the security we need, in a manageable way, while still delivering required services and enabling profitability.

But dogma plus information is not enough. At every step, senior management support is critical. From the assignment of responsibilities with authority, to the approval of purchasing, policies and plans, upper management makes or breaks the security program. Aside from the fact that in any organization senior management assigns and delegates authority, it is often the official or unofficial arbitrator should individuals or organizations disagree with policy.

The right information, mind-set, and blueprint provide the foundation for security with usability for an enterprise.

## Resources

The following books and Web sites can provide insight into the development of sound security policies and procedures.

**Books**

**Firewalls and Internet Security: Repelling the Wily Hacker,** Bill Cheswick and Steve Bellovin. Addison-Wesley, June 1994

**Designing Systems for Internet Commerce,** Win Treese and Larry Stewart. Addison-Wesley, 1998

**Web Security Sourcebook,** Aviel Rubin, Daniel Geer and Marcus Ranum. Wiley Computer Publishing, 1997

**Information Warfare and Security,** Dorothy Denning. Addison-Wesley, 1999

**+Information Security: Policies and Procedures: A Practitioner's Reference,** Thomas R. Peltier. CRC Press, Auerbach Publications, December 1998

**The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program,** Gerald Kovacich. Butterworth-Heinemann, May 1998

**Web Sites**

> **The SANS Institute, www.sans.org:** Security policies, course notes

**The Computer Security Institute (CSI), www.gocsi.com:** Various papers and editorials about security practices and products

**Project COAST (Computer Operations, Audit and Security Technology), Purdue University, www.cerias.purdue.edu/coast/:** Software tools, information archives, research projects