[**Editor's Note:** The following excerpt is from Chapter 2 of the free eBook *From Chaos to Control: The CIO's Executive Guide to Managing and Securing the Enterprise* (Realtimepublishers.com) written by Don Jones and available at http://www.netiq.com/offers/ebooks.]

Areas of Security Concern

What do you care about when it comes to security? I once worked with a regional telecommunications firm that didn't bother to seriously secure any of their file servers. They made it clear that everything on those servers was open to pretty much anyone in the company, and that anything requiring a higher level of security would need to be kept in the company's mainframe, which is where they'd invested all of their security efforts. The lesson is that you don't have to secure *everything* in your organization; you simply need to decide what you *will* secure, and make sure that everyone in your organization is on the same page.

Security Must Be Pervasive

Security is far too often treated as a separate entity and the last thing anyone thinks about. Even Microsoft used to be guilty of such behavior: Prior to Windows Server 2003, Microsoft's primary concerns were ease of use and general code stability. Security was nearly always an afterthought, implemented through minimally featured add-on tools such as the Baseline Security Analyzer.

Every new corporate project—regardless of whether it involves IT—needs to consider the security ramifications of the project. Security should *not* be implemented by some specialized department within your organization; you might have such a department, but their job should be to advise and educate other department heads. Security must be a part of every decision made.

To continue picking on Microsoft for a moment, consider the company's Win2K certification exams, which include exam objectives such as "managing file access" and "managing DNS." Near the end of the exam, there is a short collection of objectives such as "securing file access" and "securing DNS," as if those were separate topics! Newer exams correctly require candidates to "manage, monitor, secure, and troubleshoot" resources as a single set of tasks, which is exactly how things should be.

Just as every management decision must be viewed in terms of its costs and impacts on profit or productivity, every decision must also be viewed in terms of its impact on security.

Physical Security

How secure is your "physical plant?" I've already mentioned the surreptitious janitor that made off with a computer, which probably contained at least a little confidential data. Physical security is easily overlooked, in part because it's so difficult to efficiently secure. Locked doors and filing cabinets, sure, but locking computers to desks? Install paper shredders every 30 feet? Encrypting files in case the hard drive is stolen? Each of these measures is reasonable in the right circumstances; you'll need to decide when those circumstances are your own.

From a policy standpoint, you need to express in writing what you feel are reasonable vulnerabilities or situations. For example, you might work inside a facility that requires photo IDs and posts armed guards to ensure that the IDs are used correctly. In that case, worrying about somebody sneaking in and plugging into the network might not really be a concern. However, your company might work in a startup "incubator" in which your resources are practically public property; worrying about someone plugging into your private network might be a very real and immediate concern.

One way to approach physical security is to decide how likely it is for different threats to actually occur, and how big an impact it would be on your business if it did occur. To do so, you can use, as a starting point, a simple worksheet like the one that Figure 2.2 shows.

Physical Threat Assessment - Information Security

Threat	Likelihood	Impact	Total Risk
Access to physical network	85%	5	4.35
Access to wiring closet	20%	2	.4
Access to users' computers	100%	5	5
Access to servers in data center	10%	10	1
Access to document hardcopy	90%	8	7.2
Access to discarded document hardcopy	100%	8	8
Use of removable media to distribute info	10%	9	.9
Distribution of hardcopy outside office	10%	9	.9

Figure 2.2: Sample physical risk assessment.

In this example, each risk is assigned an impact level from 0 (no impact) to 10 (major profit threat). Each risk is then assigned a likelihood, as a percentage, with 100% being a risk that will almost definitely occur. The likelihood and impact are multiplied for a total risk factor.

For example, if someone were to gain physical access to the data center, it would be devastating, but it's unlikely to occur. The total risk is only 1 because the data center is locked and has a small list of authorized users. However, access to discarded hardcopy is seen as a high risk (8), that is almost definitely going to occur (100%), for a total risk factor of 8—on a scale of 1 to 10. That's a risk that needs to be analyzed, and perhaps new policies created regarding the creation and destruction of hardcopy materials.

Notice that the distribution of hardcopy by employees is a high risk (9) but the likelihood is seen as low, just 10%. That's the type of statement you can only make with proof to back it up, such as routine background checks on employees or an aggressive personality risk assessment as a part of your hiring process. The total risk factor, less than 1, means it's not something you need to do anything about; however, there's a lot of trust in that 10% rating that needs to have some business justification behind it.

Data Security

Data security is often easier to grasp than physical security because it's the type of information security most organizations are used to dealing with. Organizations that enjoy a high rate of security success often attribute their good fortune to careful planning and careful categorization of their data. Security measures can be expensive and can impact productivity; by carefully organizing data, you can minimize costs and impact across your organization. For example, you might classify your data as follows:

- User data—This categorization often includes personal files created by users as well as working documents, such as meeting agendas. In the past, many organizations secured this data so that only administrators and the specific user could access it. However, doing so creates a legal "reasonable expectation of privacy," making it difficult for businesses to legally access that information when needed. As a result, most organizations now provide no protection for users' "home directories," specifying that sensitive information be kept in other locations.
- Public data—This information is already accessible to the public through some channel, such as press releases and sales brochures. Because the information is already public, there's little need to protect it with special measures.
- Confidential data—This data is the run-of-the-mill information that isn't publicly accessible but wouldn't cause great damage if it were leaked. This information can generally be protected simply by authenticated access, and you might prohibit users from keeping local copies on their desktops or laptop computers.

> ☞ Stopping copies is the key. You might have a vast body of data that you want your employees to have access to but that you don't want spread around. Traditional computer security systems have simply granted users the ability to read a document; once they've opened it, security stops and the user can save as many other copies as he or she desires. The advent of digital rights management (DRM) promises to help stem the tide by allowing users restricted permissions to documents, such as the ability to read a word processing document but not to save additional copies.
>
> DRM only works in conjunction with rights-aware applications, such as Microsoft's new Office System 2003, which includes basic DRM functionality. Traditionally, DRM has focused primarily on stopping the spread of commercial music and video works; this extension into business information management promises to help create more secure environments in the future.

- Sensitive data—This data is information that would cause moderate damage if leaked outside the company but is generally accessible from within the company. Ideally, this data should be stored only on secured file servers or other centrally managed assets; local copies on users' computers should be encrypted in the event that the computer is stolen.
- Secret data—This data would cause tremendous damage if leaked and is not in general circulation within the company. This information should always be stored on encrypted volumes, both server-side and client-side. Transmission of the information across networks should be encrypted.

By clearly categorizing your data, you can specify service levels that define how the different types of data must be protected, and document specific threats to each category of data that are of particular concern. This type of documentation can help drive security testing and development.

Top 10 Overlooked Security Vulnerabilities

Where is security missing within your enterprise? Security management might seem like a pathological case of paranoia. However, nobody would think it odd for a business to ask "How will this help the bottom line?" at every turn; businesses aren't any crazier for trying to anticipate security problems. To help you get in the right frame of mind for security, the following list offers the top 10 commonly overlooked security vulnerabilities:

- Hardcopies—How much money do you spend securing electronic data only to have users print it out and leave it lying around for any passerby to pick up?
- Phone lines—The easy way for users to get data off the corporate network without drawing suspicion: a quick call on their laptops' built-in modem and they can send data to anywhere in the world, right from their desks.
- Network wiring—All someone has to do is plug in and start pulling traffic from the network. Are your wiring cabinets locked? Do you have live network jacks in the lobby? Who controls the provisioning of new jacks? Are there unused cubes and offices equipped with live jacks that an intruder could use unobserved?
- Physical computers—Who needs to hack your network when they can pay the janitor to make off with an entire computer?
- Firewalls—Sure, they're secured from the outside, but most corporate espionage comes from the inside.
- Printers—Getting back to the hardcopy issue: how much of your secure data lies around in the printer's output tray or in the letter bin next to the printer waiting for a user to come claim it?
- Administrator user accounts—Sure, everyone knows they should only use those accounts when they're actually administering, but the reality is that they use these accounts to log on all the time. Can you even tell what they did with their administrator accounts?
- Removable drives—Most high-end servers have them—hot swappable and everything. All someone has to do is flip a lever or two, pull, and stuff the booty into a gym bag. Not saying an intruder could access that hardware, but how up to date are your background checks on the folks who have server room access?
- Remote offices—Maybe headquarters is in order, but smaller field offices are the most likely target for an intruder trying to gain physical access. WAN lines are rarely secured and can often be accessed from outside the building.
- Unpatched servers—This security hole is a particularly common yet often overlooked vulnerability. The Slammer virus didn't make short work of SQL Server computers worldwide because of a security hole. The virus was successful because nobody had installed the patch that had been available for almost 7 months.

Start fixing these less obvious security problems and you'll be well on the road to maturing your security management technique. Many times, the fixes will have to come through new policies: lock computers to the desk, get control over network and phone lines, and write down clear policies about how hardcopies are to be handled.

[**Editor's Note:** This content was excerpted from the free eBook *From Chaos to Control: The CIO's Executive Guide to Managing and Securing the Enterprise* (Realtimepublishers.com) written by Don Jones and available at http://www.netiq.com/offers/ebooks.]