

## Taking a Proactive Approach to IT Network Security...

### Got Access?

#### *A Proactive Approach to IT Network Security*

By David Wininger, Chief Security Officer  
Systems Engineering, Portland

Most small-business owners don't think their companies' IT networks are at risk for break ins. Hackers only target big companies, right? Unfortunately, small businesses are just as likely to be targeted for a network break in.

Fact is, the potential for a security breach -- and the resulting bad publicity for your company -- is high. As a result, you must have a plan to protect confidential data such as employee social security numbers, customer credit card information and other confidential data.

What's a small business to do to protect its IT network from intrusion?

The answer is good planning. To properly manage and control IT networks, IT managers need a framework around which to build sound policies and procedures. It is this framework that provides clear data management security procedures so that financial reporting can be delivered to stakeholders accurately and with confidence. In short, secure, flexible and process-driven IT systems are essential to maintaining the integrity of the enterprise and the company.

Today, the largest threat faced by companies and organizations is not from outside attacks, but rather its own employees, vendors or consultants who have internal access to systems.

Having policies and procedures in place that better align business needs with IT responsibilities is critical to reduce this threat. Consider this: If the end result were to capture or corrupt customer data, credit card information or financial statements, would it be easier to get this information from a huge, national company or from a small business that may not have the resources to protect its information?

Along the same lines, wouldn't it be easier to divert money from a business account if you were the only one who had access to the books, rather than if there were checks and balances in place to monitor how revenues and expenses are tracked and confidential information is maintained?

Applying a framework for data management provides companies and organizations with sound procedures and processes that will reduce the threat from both external and internal attacks. The first step in the process is to document and evaluate your existing policies and procedures regarding IT security.

One way that companies can create policies and procedures for IT security is to consider the Sarbanes-Oxley Act of 2002. Known as SOX, the act -- which was created in response to corporate scandals such as Enron and WorldCom -- sets mandates and requirements to make sure financial reports are above the board. At the same time, SOX represents a standard that every

company can follow to ensure that the way they keep their books is in line with best practices found in other, larger organizations.

Additionally, the federal government, state municipalities and other large institutions are making SOX compliance a requirement to bid on their contracts. If you want to do business with these agencies and organizations, either now or in the future, SOX compliance is going to be mandatory.

And although there is no specific mention of IT security in the SOX mandate, it does include a passage stating that corporate executives must be responsible for establishing and maintaining internal controls. So even though there's no specific mention of IT security, businesses are required to maintain internal controls, and policies regarding information access.

Unfortunately, even with all of the positive advantages to becoming compliant, it may surprise you to learn that a very small percentage of organizations in Maine actually are SOX-compliant today. This is a potential crisis waiting to happen.

So, let's talk about how working towards SOX compliancy can help companies develop sound network security policies and procedures.

First, companies should establish and document a clear process for terminating access to such things as internal systems, VPN accounts and email when an employee leaves the company. The same goes for vendors and consultants with similar access: When a specific project is completed, make sure those people can't get to your confidential information. Ask yourself whether your company has policies and procedures in place to control your vendors and consultants. Whose responsibility is it to manage those relationships?

These are just a few of the types of items that a compliancy overview and IT security audit would cover.

Other things to identify include determining your ability to monitor and control network traffic, linking your systems with partners, virus scanning and operating system access controls. Organizations also need to determine how frequently to hold process reviews, and establish a system of checks and balances to identify gaps in policy and procedures, as well as other potential threats from both internal and external entities.

For many reasons, it makes sense for all of Maine's growing organizations to take a more proactive stance on IT security and taking that first step of developing a process framework. The sooner you start, the sooner you will reap the rewards of running your business a little smarter, faster and a lot more securely.

*David Winger is Chief Security Officer of Systems Engineering.*

*Mr. Winger has 25 years of experience in IT Security with an extensive base of military, government and executive management experience. [dwininger@syseng.com](mailto:dwininger@syseng.com)*