STRUCTURAL BUILDING COMPONENTS MAGAZINE
May 2003

You're Online: Is Your Data Safe? Four Steps You Can Take to Shield the Back Office by Alan Kosse & Dan Vogt

Securing your confidential data while traveling the Internet is key. Discover the necessary steps to make absolutely sure your data is protected.

Understanding how to keep data that's streaming across the Web and within an organization's walls safe is an important issue many within the structural building component industry find confusing and too easy to ignore. You shouldn't.

New abilities in Internet connectivity permits traveling employees to tap into their day-to-day business software from virtually anywhere with a PC. Cyber cafes, motel rooms and branch locations are common dial-up ports today for data retrieval. But how protected is the data you're accessing?

Building component manufacturers and distributors should ask themselves if they've taken at least fundamental steps to keep important information within their network confidential and unexposed. The first step is to admit Internet security poses a potential problem. The second step is to identify a level of security protection appropriate for your business.

Whether you're among a few innovative distributors who have already moved to an Application Service Provider (ASP) business management computing model, or if you maintain a traditional in-house system, computer security can be simple. With the ASP, or "hosted" model, which includes outsourcing software and hardware, advantages are inherent.

For example, in an ASP environment, your computer screen is essentially a window into an off-site, tightly guarded bunker where your IT network and data reside. Your PC becomes a remote tool that can safely select back-office software controls behind a secure zone. In this way, back-office data remains shielded, moving less frequently across phone lines.

It's this "secure zone" that's the bread and butter of the ASP model, meaning IT and software maintenance can be performed more efficiently than many small businesses can do alone. Data centers provide the physical security that keeps hardware servers running around the clock. This includes temperature controls, fire retardants, backup power, surveillance and security breach alarms. But also, the ASP model offers data corruption and denial-of-service protection to help keep access in the hands of the right people.

BUILD A MOAT AROUND YOUR CASTLE

To build similar protection into traditional IT systems held in-house, component manufacturers

and distributors should consider “firewalling” to safeguard data within their Local Area Network (LAN). A firewall filters data coming-from and going-to the Internet and offers protection from hostile intrusion like a moat around a castle. To enter your castle, there should be a drawbridge, or password. Firewall packages can come in the form of hardware or computer installed software starting at about $200.

But whether your business follows the ASP method or keeps computing systems in-house, the policies that guide your security system are equally important.

IMPLEMENT THE “80/20 RULE”

A small, family-owned component manufacturer or building products distributor may or may not be the highest risk place for computer hackers to steal information or cause disruption with viruses, etc., but it can happen. The majority of problems actually come from inside a company. This explains why you can solve 80 percent of computer security issues with 20 percent effort.

The 80/20 rule includes four easy steps:

1. Change your passwords. Whether you have a $100- or a $100,000-firewall solution, the greatest protection comes by regularly changing your system passwords. Logon passwords should not allow you to re-use the same password for an extended period of time. Consider having passwords reset every 60 days.
2. Create distinct passwords. To make passwords more difficult to decode, build in logic and try mixing numerals with alphabet characters.
3. Log off your PC. Do you lock the door to your home or car? Most people do, but fail to consider the opening that's available to would-be corrupters when an office PC is not shut down. Unless you do this, access to important files across an entire network, email and other documents can be too easy.
4. Determine administrative rights. Get your business in order. Who has computer network administrative rights within your company? Do only a few people have power to control the gateway into your network? Do they employ appropriate measures to block their access to files after employees leave the company? Firewall settings can be changed to allow certain executives to dial into the office from the road; can be used to limit in-coming and out-going email; and limit Internet access.

The newest technical aspects of ensuring safe, consistent streaming Internet services can vary by worksite. Component manufacturers and building product distributors interested in learning more about business interruption insurance and planning should consult a security professional.

Internet technology will continue to evolve, and as it does new security issues will arise. But, if you can pay attention to the fundamentals that can deter corruption yet keep your staff informed while they're traveling, you'll be assured of a more secure, efficient business.

Alan Kosse is a Marketing Communications Specialist at Distribution Management

Systems, Inc. Dan Vogt is DMSi's Vice President of Customer Services.

SBC HOME PAGE

The mission of Structural Building Components Magazine (SBC) is to increase the knowledge of and to promote the common interests of those engaged in manufacturing and distributing of structural building components to ensure growth and continuity, and to be the information conduit by staying abreast of leading-edge issues. SBC will take a leadership role on behalf of the component industry in disseminating technical and marketplace information, and will maintain advisory committees consisting of the most knowledgeable professionals in the industry. The opinions expressed in SBC are those of the authors and those quoted solely, and are not necessarily the opinions of any of the affiliated associations (SBCC, WTCA, SCDA & STCA).