So You Thought You Were Protected And In Control

Utilizing A Few More Ounces Of Prevention For Your IT Assets

by Robert Stuckey and Kenneth Cooper

Firewalls, routers, passwords, anti-virus software, etc...Protecting your information technology (IT) assets and processes is both time-consuming and expensive. The "smallness" of a business can result in a false sense of IT security. Small organizations are more at risk than large enterprises because of "all the eggs in one basket" and the potential for lax security and backup procedures.

The following is a guide to selecting the right business controls for your data processing investment by highlighting IT business exposures. Notice we use the term "business controls," not internal or financial controls. Five questions to ponder from the business controls perspective are:

1. Just what should I protect?
2. How many layers of protection are needed?
3. What resources are needed for protection?
4. What is the frequency(ies) of protection?
5. Do I need protection redundancies?

Exposures to the "normal" elements of the technology function are always a challenge. IT obsolescence, changing employee skill sets, and equipment reliability are all valid concerns that can affect your success. Layer in those "intentional" detriments like viruses, hackers, etc., and you have a total business exposure independent of items you may think you have under control.

Just What Should I Protect?

In addition to devices that physically protect hardware, such as surge suppressors and network equipment, software needs its share of protection with anti-virus products. For example, one local IT small-business consulting firm received 70 panicked customer phone calls in its first hour of business the day the Michelangelo virus became active. By then it was already too late for those 70 businesses.

Employee turnover can unnecessarily expose data to either unintentional or malicious corruption. In one example, before a fired employee left the premises, he corrupted critical data requiring thousands of dollars to reconstruct. A preventive procedure is to cancel access immediately for any employee being terminated. (Note: *Any* anticipated change in the composition of the workforce should raise a red flag for a potential disruption in stored data.)

How Many Layers Of Protection Are Needed?

Initially, a logon password to the computer was adequate. The next step was to require a personal password for access to the software on the equipment. With the advent of networks, regardless of size, a network password became necessary. With the proliferation of the number of systems on the network, and the sensitivity of the information on these systems, an individual system or application password has become necessary.

In businesses with only a few employees, it is not uncommon to disable the password requirements. This puts data at risk. The levels of access control must match sensitivity of the data and the availability of the computers. This often requires layers of security. For example, with any computer that has portability like a laptop, multi-layer passwords should be implemented. While many people think that computers are frequently stolen from office buildings, theft of a laptop in an airport or train terminal is a more likely prospect.

A word of caution: "Small" is no excuse to minimize multiple layers of protections. Review your security and backup procedures regularly.

Resources Needed For Protection

There are ample choices for hardware and software protection. However, one of the most important resources that is overlooked or taken for granted is the human factor. How people use the hardware and software is your last line of defense. For example, as companies migrate toward the Internet (i.e., e-business) there are a host of exposures unique to that environment.

In addition to anti-virus software, educate your people about Internet scams. The Internet is also full of advertisements and "good deals" that just require the company's credit card number. People can easily get sucked into downloading malicious graphics or data files, and participating in chat rooms. Even if these are nonintrusive, at a minimum the hard drive gets overloaded with electronic junk mail. This slows processing while requiring additional storage space—especially if the hard drive is backed up frequently. The moral? Make

(Continued on Page 16)

Local Companies Develop Internet-Registered Mail Software

Two St. Louis area companies have discovered the Internet's answer to registered mail—better known as gProof®. gProof provides third-party confirmation that an e-mail was sent, received and accepted at a proven date and time, and fills a void for confirmation and verification in today's fast-paced, digital environment.

gProof, which stands for global proof of document delivery, provides verification and off-site storage of e-mails, faxes and other types of electronic communication. gProof is a web-based service, enabling subscribers to send e-mail or faxes and have time-stamped electronic copies stored in a secure off-site server, proving when documents were sent and preserving contents for future references. In addition to managing corporate e-mail, gProof offers a comparable service for faxed communications.

"gProof eliminates doubt and uncertainty from electronic communications," said Dwight Homer, gProof marketing director. "It's as easy as sending a carbon copy of your message to a password-protected online account. You just 'cc' the e-mail in question to your gProof account, and you're protected from any questions as to what was sent to whom and when."

In addition to managing corporate e-mail, gProof offers a comparable service for faxed communications. gProof can time-date, verify and store faxes, which are saved as PDF files in the user's account.

"We believe this system crosses all industries, but is particularly useful for legal and contractual matters," Homer said. "For example, it would be helpful to mortgage lenders who need to confirm the timing of 'locked-in' rates or to general contractors and architects managing 'change orders' on construction projects. The scope of potential uses is endless."

gProof was originally developed by Wildfire as an in-house project management tool to help developers stay on top of changes in managing the software development process.

According to George Sykes, president of Wildfire Internet, "Web development is a fast-moving, dynamic process. Customers always want to do more and we want to accommodate them. But tracking change orders and subsequent versions got to be a challenge, so we developed gProof."

Financial Network, a firm specializing in lending decision systems for national accounts in banking and finance, immediately recognized the benefits of gProof for financial clients with security and compliance issues.

"We work with many banks and consumer credit providers, so the secure third-party tracking, storage and verification of e-mail and fax communications is incredibly valuable," said Clint Lane, president of Financial Network. "In today's quest for accountability, gProof is an great tool."

A joint venture of St. Louis-based Financial Network, Inc. and Granite City, Ill.-based Wildfire Internet, Inc., gProof is available for $5.99 per month, plus a per e-mail processing and storage fee beginning at $.25, depending on the size of the file.

So You Thought You Were Protected And In Control

(Continued from Page 15)

certain your employees know how to utilize your IT investment in the most efficient, safe manner.

Frequency(ies) Of Protection

Depending on the type of business you are in, business controls will depend on what and how often you back up. Depending on the number of transactions per day—this may be hourly, twice a day, or daily. With lower transactions, this is maybe every other day or even weekly.

A common complaint on frequency is, "This is just another thing I have to do when I should be growing my business." Fortunately, there are a number of software packages that will do backups simultaneously while working your accounts.

A word of caution: Extending the frequency to fit your timetable for when it is convenient will eventually cost your business money. Schedule it, do it, and enjoy peace-of-mind knowing that this is one less thing to worry about.

Protection Redundancies

Storing backups in a secure location is an inexpensive "insurance policy" in both protecting your critical and sensitive data, and in avoiding the operational hassles of running your business. There are a number of portable mass storage media, such as tape, external hard drive, zip drives, or CD-R discs, that can make this step easy to do on a frequent basis. The key here is making a backup process a part of the daily or weekly routine—just like opening the mail or paying the bills.

A word of caution: Having the capability to backup but doing it infrequently is like not having backup capability. Infrequent backups could cause delays in your operations because of the effort required to reconstruct the data. Likewise, regular backups stored next to the working computer, reduces the safety factor since the backup data exists in the same physical environment. One church lost five years of data when a janitor stole not only the church's PC, but also grabbed up anything that was on the table or in the desk relating to the PC, including the backup disks.

Next Steps

It is impossible to review in detail all business exposures your information systems could face in this article. However, you can take preventative, proactive measures to minimize risks. There are specialists in business controls that can assist you. Just as your business processes are integrated, you require an integrated approach to managing and improving your business controls.

Robert Stuckey (rstuckey@biz-control.biz) and Kenneth Cooper (kcooper@biz-control.biz) are partners of BizControl Solutions, a firm specializing in business controls assessment, consulting, implementation, and training.