James Kavanaugh, Comptroller and Treasurer at Parker Thompson, says internal IT security is best left simple.

WRITING A HAPPY ENDING

POLICIES AND PROCEDURES CAN PROTECT YOUR CORPORATE (DATA) ASSETS • BY KEITH CHVAL

Ask yourself which of your corporate assets you could least afford to lose: a) your company's strategic plan; b) client lists; c) new product or marketing campaigns; d) your pricing matrix.

Whatever your answer, there's an excellent chance that the assets most critical to your company reside on a computing device of some type. And the chances are nearly as good that your critical data could disappear in a matter of moments, even seconds.

"It's truly astonishing to see what businesses are grappling with in terms of the depth and breadth of vulnerabilities and liabilities thrust upon them because of the aggressive implementation of technology within all areas of operation," says Cathy Kiselyak Austin, chair of Chicago-based law firm Gardner Carton & Douglas's intellectual property department. "The challenge is magnified for smaller businesses that often are not yet at a point where they can have employees dedicated to these issues."

Worse still, employees are often to blame for data loss in the first place. Every day, hundreds of small businesses wake up to find that one of their own has accidentally or intentionally walked off with sensitive information, such as sales data. According to the Computer Security Institute/FBI 2005 Annual Computer Crime and Security Survey, insiders account for half of corporate computer security breaches, costing victimized businesses $204,000 on average.

What can you do to avoid becoming a statistic? Create manageable data-security and technology-related policies and procedures to significantly minimize technology's inherent risks and harms.

An Ounce of Prevention Outweighs a Pound of Cure

The primary goal of data security policies and procedures is simple: fewer and less severe incidents. But when an incident occurs, you typically have four options: investigate and put an end to the conduct, handle the incident as an internal or administrative matter, pursue legal recourse through the civil justice system, or refer the matter to law enforcement for criminal investigation and prosecution.

Begin by approaching each incident as a criminal matter, at least in an investigative sense, says Austin. Because criminal prosecutions require the highest degree of proof, ***remember that part of your goal is to build a case that can be criminally prosecuted.*** By doing this, you preserve all your options while you gather all the facts.

This requires strict investigative procedures. Evidence must be properly collected and handled so as to not only meet the requirements for admissibility in court, but also preserve its greatest persuasive value.

"Unfortunately, in more instances than I care to remember, I have had a small business owner or executive come to me without legal recourse after an incident has occurred, whereas, had we done some work on policies and procedures up front, they could have been in a strong position to vigorously pursue their legal rights," says Austin. "There is no worse feeling as a lawyer than to have to explain to a prospective client that, 'Yes, I agree that what this person did is really terrible, and could otherwise be actionable, but we simply do not have the requisite legal basis to pursue them because they technically did not do anything that violated their terms of employment."

David Haslett, chief of the Illinois attorney general's High Tech Crimes Bureau, says two areas almost always serve as stumbling blocks in its pursuit of employee wrongdoing. The first is that law enforcement is unable to

80% of small businesses exhibit confidence in their existing information security practices; **56 percent** have experienced one or more security incidents in the past year; and **74 percent** do not have an information security plan, according to a 2005 survey by the Small Business Technology Institute.

CHRISTOPHER NAVIN

collect critical electronic evidence, such as e-mails or electronic files, from a target's work computer because the employer does not have an acceptable-use policy that authorizes them to turn over files. ***If your company allows employees to develop a "reasonable expectation of privacy" it may preclude law enforcement from viewing that evidence.***

The second common stumbling block is that law enforcement needs to prove that an employee accessed electronic files without authorization. "This typically requires that a policy and related procedures previously be in place which clearly set out the limited purposes and conditions under which that individual was allowed to have 'authorized' access and use of that system or file, and that the employer also enforced those policies," explains Haslett. ***Unfortunately, clearly defined and enforced policies are "rarely" in place***, Haslett warns.

The Policy Design Process

That can be changed by designing and implementing data security policies and procedures with the full support of all senior-level management, including the CEO. In fact, a typical policy document begins with a statement of CEO support.

After gathering the senior management project team, with input from all the company's operational areas, carefully assess the corporation's operations to identify areas of risk and vulnerability. This must include considering legal and regulatory compliance requirements. The participation of legal counsel is essential. This assessment will allow the corporation to focus only on assets and vulnerabilities that truly are critical, while avoiding unnecessary policies and bureaucracy.

Once the assessment is completed, policies and procedures can be drafted. Unless the expertise and resources reside in-house, this is one area where utilizing outside expertise usually makes sense. Wherever you turn for help, the policies and procedures you create must be comprehensive — providing for the prevention of, detection of, and response to an incident. They must also be collaborative — to include all operational departments of your business, even outside vendors, if they play a key role in operations. And they must be evolutionary to account for new technologies. The absence of any of these characteristics will ultimately lead to the failure of your efforts.

92% of company documents are stored in digital format (University of California at Berkeley survey). **69 percent** of business professionals have stolen some form of corporate Intellectual Property ("IP") when leaving the company, the most common method — sending copies to a personal e-mail account (Ibas Corp. survey).

The security challenge is magnified for small businesses without dedicated security personnel, says Cathy Kiselyak Austin, Chair of the intellectual property department, Gardner Carton & Douglas.

JOHN NEUBAUER

While easy to overlook, security policies and procedures must keep pace with technology. Consider, for example, cell-phone cameras and instant messaging. ***Take advantage of file server controls to restrict and enforce access, but make sure the restriction is documented and signed by employees.***

For example, Jeff Bowden, a security expert and IT manager at Delmia, an Auburn Hills, Mich.-based subsidiary of manufacturer Dassault Systèmes, suggests restricting employee access to certain files. "Small businesses generally give full access to all data to all employees. While this makes administration and file access easier, it also compromises security," says Bowden. "Take some time to set up file access so that employees can see only files that they need to."

Also, don't allow personal customer information, such as e-mail addresses, credit card information and Social Security numbers, to be stored on a notebook computer or removable device, says Bowden. Reset company notebooks so they require user passwords to access hard drives and the system's BIOS (basic input/output system). The BIOS is the program your computer's processor uses when you boot it up — without it, data on it cannot be viewed easily.

James Kavanaugh, comptroller and treasurer at Parker Thompson, a 150-person construction management firm in East Providence, R.I., finds internal IT security for small- and mid-sized businesses is best left simple. "If you make it too complicated, no one uses it," says Kavanaugh.

That's why Parker Thompson employs two basic internal security measures: Microsoft's Active Directory and GPOs, or Group Policy Objects. Active Directory, a feature of the Windows operating system, allows administrators to determine which users get access to which files. GPOs are collections of such user-settings and work in tandem with Active Directory. "One GPO we did was to have computers automatically lock after five or 10 minutes of non-use," says Kavanaugh. "We noticed that people will get up from their desk and walk to another part of the office. If they leave the computer logged on, they leave it logged on with all their access privileges. That could be a problem, especially if those computers are in the accounting or payroll department."

What to Include in Your Policies

Granted, what works for one company may not be the right fit for another. But consider the following questions when forming your policies and procedures:

Control of Information and Assets

- Identifying confidential information: What documents and materials require protection and how are they going to be identified as such?
- Controlling access and use: Who will be allowed to access identified materials? How is access limited? What are approved uses of the materials?
- Release of information to third parties: What information may be shared with third parties and under what conditions? Who has authority to release what?
- Audits and controls: Do you have an inventory of your tangible and intangible assets, including software licenses? How will you track the location of these assets?
- Off-site storage and access: What tangible and intangible assets will employees be allowed to access off-premises and under what conditions?
- Use of personal property: Will employees be allowed to use personal devices such as PDAs and removable USB drives for corporate purposes? What rights, if any, does the corporation have to control their use and inspect them?

Prevention and Detection

- Use of technologies and applications: What prevention technologies will be used? Who will be responsible for updates and patches for all applications deployed by the company?
- Third-party visitors to physical plants: Are there any limitations as to where visitors can go? Must they be escorted? Are visitors precluded from bringing particular items such as PDAs, cameras or portable storage devices onsite?
- Acceptable use and privacy: Are there any limitations on personal usage of corporate resources and technology? Should employees have any expectation of privacy for personal materials located or used on corporate property? How will employees be informed of the policy?
- Monitoring electronic communications and Internet usage: Will this be done and for what purposes? Who will be responsible? How will employees be notified?

Incident Response

- Chain of command: Who directs the response and investigation? What responsibilities and authority do various managers and departments have?

According to the Association of Certified Fraud Examiners, U.S. organizations lose an estimated $652 billion to fraud, with 42 percent occurring in companies with fewer than 100 employees.

- Notification: Who must be notified internally and within what time frame? Under what conditions must or can law enforcement or regulatory agencies be notified?
- Response and investigative personnel: What skill sets are needed? Identify in-house personnel with necessary backgrounds and training, and outside sources for skills not present in-house.
- Investigation protocol: Should an "offender" be interviewed or confronted immediately, or should additional evidence first be collected? Who conducts the interview? What skills should interviewers have?
- Preservation, collection and handling of evidence: How can you ensure that server logs and deleted data are not permanently destroyed? What collection, handling and storage procedures will be used to preserve evidentiary value?

Making IT Work

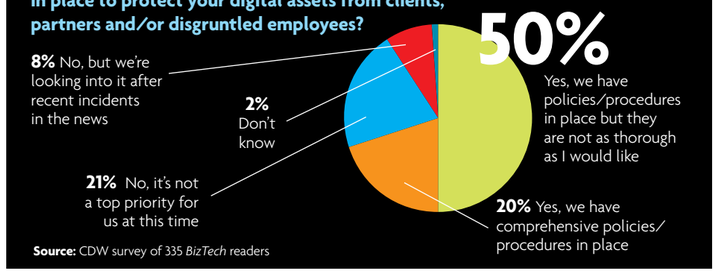
Once your policies and procedures are completed and adopted by management, give them life by effectively communicating them and building employee buy-in and awareness of their critical importance. Consider, too, the tremendous deterrence that awareness of your corporation's commitment to data security will have on security threats.

"As the saying goes, 'You're only as strong as your weakest link,' and nothing could be more true in the world of technology and information security," cautions Jon Tegethoff, a project leader with Protek International, a Chicago-area computer forensics, investigations and litigation services firm. "You can deploy the latest and greatest technologies and design and implement wonderful policies and procedures, but it's that one employee who really doesn't get it, or just isn't onboard with the program, who's going to compromise everything that you've done." [BT]

Additional reporting by Kevin Ferguson

BizTech Quick Poll

Does your company have formal policies and procedures in place to protect your digital assets from clients, partners and/or disgruntled employees?



Source: CDW survey of 335 *BizTech* readers