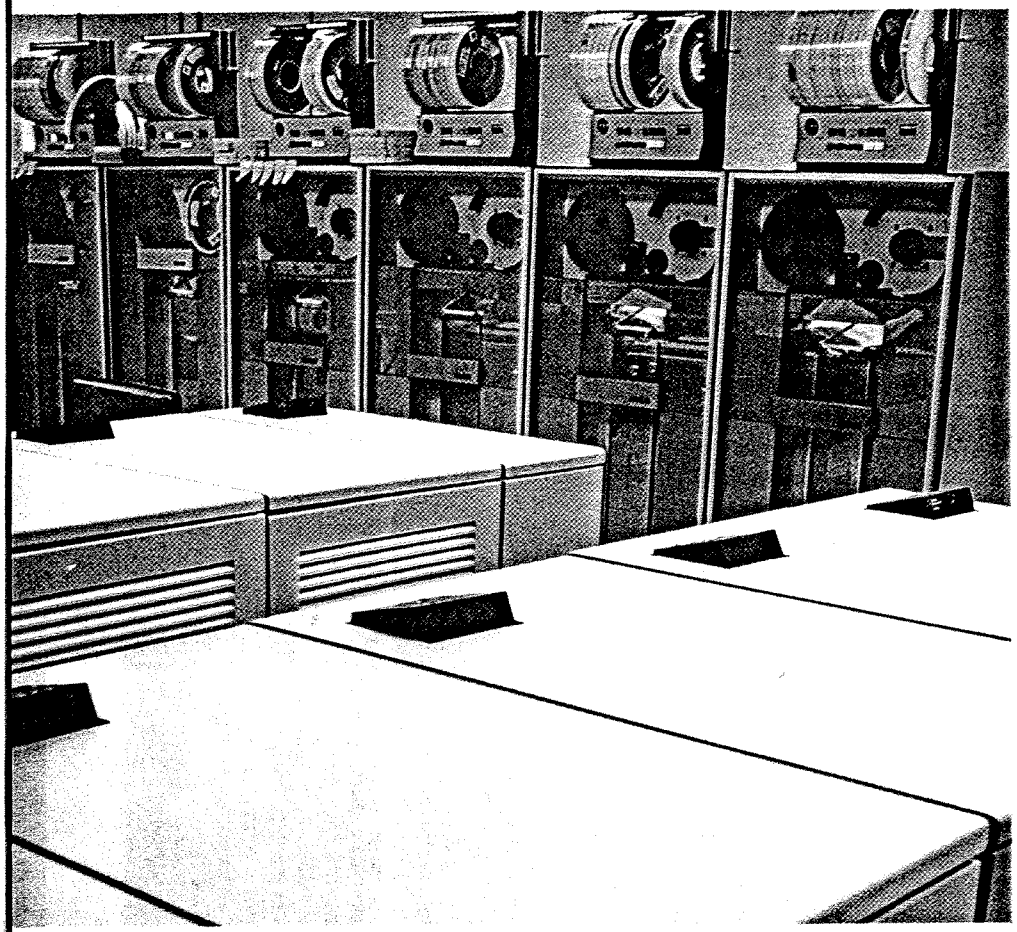
Employers Beef Up Cyber Security to Better Protect Payroll Data



BY PHILLIP M. PERRY

Payroll departments are undergoing a paradigm shift in communications.

Not long ago their biggest challenge was figuring out ways for widely scattered company departments to share personnel records embedded in central mainframes. Today, with computer networks offering a dream-like ease of access, the challenge is quite the converse—how can social security numbers, direct deposit information, home addresses, passwords, and salary levels be protected from the wrong people?

Protecting Payroll and Personal Data

That question goes to the heart of a more threatening security environment.

"Protection of payroll data is something that employers should be particularly concerned about, given all of the recent problems with identity theft," said Maria Perugini Baechli, a shareholder at Littler Mendelson, a national employment law firm.

Recent headlines have added fuel to the identity-theft fire. Time Warner, Inc. reported in May 2005 that the company lost the social security numbers and other personal data of some 600,000 current and former employees and relatives when a storage company misplaced computer backup tapes. Around the same time, massive breaches of consumer data were reported at Citigroup, Bank of America, MCI, and two major credit-card processing organizations.

Such events, along with an overall escalation of reported identity theft, have spooked the public and sparked federal and state laws penalizing companies negligent in the protection of employee data.

"Outside of financial institutions and credit bureaus, employers are probably the keepers of some of the largest collections of personal information," said Tena Friery, Research Director of the Privacy Rights Clearinghouse. "Their databases contain names, social security numbers, addresses, relatives' names, and even health information."

Of the harsh penalties experienced by employers who lose data, not the least is the decline in workplace morale when employees feel their personal information is not secure. And, of course, there is always the possibility of legal action if employee information is leaked or stolen.

Identify Sensitive Data

The first step in protecting data is determining what information needs to be kept under lock and key. Not all information is private enough to warrant a high level of protection, and companies cannot afford to protect everything. So what data should be secured?

"Certainly, in terms of risk assessment, social security numbers are at the top of the list of what to protect—along with other data that can be used in identity theft such as direct-deposit bank account numbers, home addresses, and driver's licenses numbers," said Donald Harris, President of HR Privacy Solutions, a management consulting practice that assists companies in addressing privacy challenges.

Harris offers the following examples of common risks, and the data that needs to be secured to avoid each:

- **Loss of trade secrets and company financial information**—External parties who get hold of payroll data can use it to obtain competitive information through a technique called "social engi-

neering," which involves tricking current employees into revealing data over the telephone or by e-mail.

Data to protect: employee and department ID numbers, names of individuals to whom employees report.

- **Internal disputes**—Confrontations can arise among employees when they perceive compensation disparities as a result of leaked payroll information.

Data to protect: wages, bonuses, options, hours worked.

- **Lowered morale**—Confidence in the company can drop when information is leaked about personal data that an employee may perceive as sensitive.

Data to protect: wage garnishments, tax levies, child support payments, marital status, contributions made to charitable organizations through payroll deductions.

- **Endangered future**—An employee's credit standing or ability to obtain another job may be in danger when information is leaked.

Data to protect: sick leave, disability payments, workers' compensation payments, wage garnishments, tax levies, child support payments.

Establish Physical Protections

Some effective techniques to protect sensitive data include the following:

- **Lock up documents**—Control access keys and make sure the payroll premises are not easily entered. Arrange for protection from the cleaning staff in the evenings and on weekends. Paper documents with sensitive data should be stored in protected areas, and discarded documents should be shredded.
- **Limit use of social security numbers**—Many companies use social security numbers for employee identification and even as access codes when individuals log into company networks. Alternative numbers for employee identification are harder to deduce. Try to limit use of social security numbers to documents filed with the IRS and the Social Security Administration.
- **Limit data printed on paystubs and paychecks**—Since many employees just toss their paycheck stubs in the trash, it's wise to include only the minimum required information, such as the name and an employee identification number on the checks. California is the only state that requires the last four digits of social security numbers to be printed on paystubs. To ensure better protection, omit all of the employee's social security number on paystubs for employees in other states, since people often use the last four digits for passwords or other identification purposes.

Electronic Security Steps

1. Security experts advise creating multiple levels of security around the computerized database. The outermost one is a firewall that keeps outsiders at bay. Just inside is a password system that allows only authorized employees to access specific categories of information. Inside that, is a layer of encryption that keeps sensitive data from being seen by anyone without a software key.
2. Many of the new state laws addressing the security of employee data free employers from liability when digital files have been encrypted.
3. Establish access rules. Security experts suggest limiting the collection, use, and disclosure of sensitive data to the minimum necessary for the intended purpose.
4. Bank account numbers should be available only to individuals who are involved with the direct-deposit activity. Once rules are established, install software that maintains audit trails of who attempts to access, change and delete data.
5. Perform background checks on payroll staff.
6. Control data entered on PDAs, laptops, or paper documents. The increasing use of laptops and other technological devices means more employees are taking work home or taking it along on business trips. In both cases, it is easy for sensitive data to be stolen along with the laptops or BlackBerries themselves.
7. Close up security holes created when employees depart. "Upon terminating an employee with authorized access to sensitive data, promptly change all passwords and security codes available to the terminated employee and require the immediate return of computer disks, compact disks, other storage devices, keys and laptop computers," Baechli said. "After terminating an employee with authorized access to sensitive data, strip the employee's computer of sensitive data before reissuing the computer to another employee."
8. Monitor access by vendors. Bar temporary, outsourced, and vendor employees from sensitive data except when absolutely necessary.

"It's not uncommon for organizations to set up Web-based interfaces for payroll processing," says John Kiser, CEO of Gray Hat Research Corp., a security consultancy. "Many times that Web-based system does not belong to the company that provides the interface, but sits in some Internet service provider data center."

Kiser suggests taking a hard look at any external organization that houses employee information as such systems are subject to hacking.

Blanket Approach

A successful program to protect payroll data will combine techniques that address physical documents, computer files, and employee practices.

"While many employers have started to make needed changes in their internal practices, payroll data protection is still a work in progress," Baechli said. "Companies need to remain flexible, responding to new problems and technological advances." ŏ

Phillip M. Perry is an award-winning journalist who has been published widely in the fields of business management and law.

New Bill Would Protect Employee Data

New federal and state legislation is raising the heat under employers. Perhaps the most important law is the Personal Data Privacy and Security Act of 2005, now under consideration by Congress.

One of the main provisions of this proposed legislation is that in the event of a security breach, employers have to notify individuals about what information has been stolen.