TECHNOLOGY

By Al Doran, CHRP

PROTECTING OUR HR SYSTEMS FROM DISASTER

The tragic events of Sept. 11, 2001 have given us all good reason to review the security of our human resources management systems. Organizations rely on the information in their HR systems to conduct business and meet regulatory and contractual obligations. That very dependence on this information should compel us to take a serious look at our security for protecting this valuable asset and our contingency plans in the event of a disaster.

Why have a plan in place? Well, quite clearly the vital information contained in our business systems is becoming more vulnerable to risks. Corporate Web sites are being hacked and assaulted with the end result often being a "denial of service." Employee information is exposed when hackers can access corporate systems. Computer viruses infect systems on a regular basis. There is a threat of cyber-terrorism that now seems more realistic than we might have imagined.

What will you do if disaster strikes and wipes out your headquarters and all your computers? Will you be able to institute a contingency plan that includes a full back up of all your essential HR data? In today's almost paperless business environment, it's essential that we have the ability to carry on in the event of a physical catastrophe.

While the chief information officer (CIO) of your company may hold overall responsibility for the security of corporate systems, individual managers also have a responsibility to ensure they are aware of security procedures and, in fact, are part of the plan to protect the information they are responsible for. The senior human resource person is responsible for the security of the information on the corporation's employees.

Senior HR managers know that the accumulated information in their HR systems represents a knowledge base that supports the organization's success, and cannot be easily replaced. Now, third-party suppliers, off-site employees and contractors, and unfortunately on some occasions, thieves and vandals have unprecedented access to this information via networks. Information security risk has increased in proportion to the number of people in a position to compromise the confidentiality, integrity and availability of an organization's information.

What is the degree of risk?

The degree of information security risk may vary from one organization to another. The first thing to understand is the level of risk that the organization is facing. One of the best ways to do this is through a formal Threat-Risk Assessment. At minimum, an assessment should provide the senior management with a complete inventory of the information assets, the absolute financial and relative value of each asset, and the vulnerabilities of each asset to risks. The relative value must consider the potential costs to replace the information if it is lost.

There is no such thing as a perfectly secure system in today's e-business world. There will always be a certain amount of risk involved in managing human resources information in this environment. The organization must decide which risks are acceptable and which are not. There must be a plan to reduce or mitigate risks that are not acceptable.

How to continually minimize and reduce risk

- Promote the active pursuit of systems security and employee use policies.
- Monitor and account for all changes to the business that may affect security.
- Raise internal awareness of systems security and risk to the company among all employees through regular security awareness programs and easy access to policies and procedures.
- Ensure that all new systems meet a rigid set of requirements before they are purchased and implemented.
- Have a contingency plan that includes a back up of all your essential HR information at a separate site.
- Perform regular audits of the organization's systems security by independent sources.
- Know whom you are hiring and who is allowed access to your systems.
- Develop and maintain close relationships between business units, systems operations, telecommunications, physical security, human resources and others in the development and ongoing improvement of the corporate security plan.

Another important obligation of senior management is compliance with legal and regulatory requirements. Since information systems are often used to manage compliance data, HR management must have a solid understanding of both the regulatory requirements and the compliance systems. Canadian privacy laws now restrict how organizations may use personal information. Organizations that break this law, intentionally or otherwise, face several substantial risks including damage to reputation, litigation and/or enforcement actions, disruption of operations, and even failure to achieve their strategic goals. HR management must be thoroughly familiar with this new law, and with the security measures that protect personal information on their systems.

The consequences of a crisis are difficult to identify without looking at them on a case-by-case basis. Some of the consequences to consider are legal actions by employees and/or bargaining units. As well, the loss of critical human resources information may greatly impair the organi-

zation's ability to operate. The failure to meet basic risk and business management principles can lead to more trouble than it's worth.

HR managers need to realize the value of security, but even more importantly they need to understand the consequences — to themselves and their organizations — of failing to properly protect their information systems. □

Al Doran, CHRP, is president of Phenix Management Int'l, a Toronto management consulting firm specializing in HRMS issues. He is co-author of a new book published by Carswell, Human Resource Management Systems: A Practical Approach *(www.hrms-book.com). Doran is a past president of IHRIM and sits on the board of directors of both IHRIM and CCHRA. He recently edited the new IHRIM Press book*, E-Work Architect: How HR Leads the Way Using the Internet *(www.ihrim.org). He may be reached at aldoran@pmiHRM.com and his home page is www.pmihrm.com.*