

Determining the Risk Involved in HR Technology

Alfred J. Walker, Senior Global Advisor

HRIT Risk Perspective

In the wake of Sarbanes-Oxley legislation, and losses of sensitive financial and personal data from well run companies as well as government agencies, and daily threats from outside computer viruses, it is no wonder most of us have risk on our minds. This is especially true for small or mid-sized companies involved in the global marketing, production and sales of products and services. And we must deal with that risk on a daily basis, not only from a business sense, but also from a personal perspective, given the 9/11 attacks; devastation from major hurricanes such as Andrew and Katrina; a multitude of tornado strikes; threats and intrusions from disgruntled employees or groups such as PETA, and kidnappings especially in South America and Europe. So in addition to protecting or HRIT investments, the depth and breadth of the risk discussion must include the safety of the human resources of our companies since people must be protected at even a higher level from danger and intrusion than our more fixed assets.

Size Matters

Size of company may matter on this issue, for several reasons. First, larger companies may have more staff to address this issue. In addition, small or mid-sized companies may mistakenly feel they are not targets for intrusions or attacks. Or, since they may outsource more of their HR operations to vendors, they may feel that it is not their job to concentrate on security. But the list of small and mid-sized companies contains many well run companies, including the likes of Celanese, Land O'Lakes, Occidental Petroleum and Google. They and others would agree risk has always been present and is clearly an issue today. We are vulnerable on a number of levels, and security of our people; their work and work place; their intellectual property; and the information about them is a major concern to all.

Historically, especially before computer technology was so prevalent, how we dealt with heightened risk from the individual physical side was with increased personal awareness, better employee identification systems, locked buildings, secured doors and file cabinets. The company response to external risk was then, and remains today, is to have adequate guard presence, more complete internal rules and auditing controls. In addition, many companies have asked for increased involvement from the insurance industry. This is because risk assessors and insurance industry underwriters have been dealing with the issue for centuries, determining life expectancy probabilities or computing the likelihood of loss due to catastrophes such as fires or floods, and pricing the premiums accordingly.

Leaving personal physical security aside as it is outside the scope of the HRIT function, in the last 20 or 30 years the issue of risk has become more complex. With the growth of technology in all its forms, especially where remote global access through networks and the Web is present, the IT function's risk analysis has had to deal with overwhelming problems such as computer viruses, hackers, spam, phishing, and spyware as well as maintaining the physical systems themselves. As

more and more firms are dependant on their on-line networks, they at the same time are increasing their risks. Financial, product, customer and supplier data are all available on a 24/7, global basis, and are increasingly open to attacks.

HRIT Involvement and Risk Framework Development

It has been a fairly recent phenomenon that we in the HRIT field have been drawn into this discussion since our systems and data, while vitally important, have not been considered by all as “mission critical”. However, it is now recognized that we are the custodians of extremely critical information on a personal, private, and business confidential level. There are categories of HR data such as compensation, payroll, pension, names, addresses, benefits information, social security numbers, bank account information, performance management and succession planning information among others on current and past employees. So for most of us, assessing risk of damage or loss to our HR data and systems has become an item on our “must do” list.

To address this issue, a framework has been developed, comprised of four major activities; identification of potential risks; prioritization and quantification of those; development of plans to eliminate or decrease the risks; and implementation of the most important issues. Perhaps you are already using this risk framework, but if not, it may assist you in your dealing with this important aspect of HRIT management.

Risk Identification

The first item in the framework is to identify the possible sources and types of risk we may encounter in our HRIT work. Since we are dealing with data and information process and procedures which are all private and sensitive, we can assume that all our data is confidential and must be protected at the highest levels. There is no one overall list of possible risks that we may face since each company and firm is different in its product lines, type of business, and geographic location, but some of the more important risks should include an analysis of possible exposures to such areas as:

- Internal data storage and security
- Access privileges, both internal and external
 - Who can access data
 - Who can alter or delete data
 - Legal issues to access
- Data change, flow, and control procedures
- Vendor data security
 - Are their procedures adequate
- IT network reliability
- Web site and self-service robustness
- HR policy and plan support
- Back-up and recovery processes
- Archival procedures
- Compliance and payroll contribution issues
- Business continuity procedures
- Data transmission processes
 - Where is it sent
 - What safeguards and controls are in place

Prioritization and Quantification

The next step is to categorize the risks and to determine the possible causes of risk and how potentially important they are in terms of loss and the impact of these to our operations, the organizations, and the staff. These activities include discussion around issues such as:

- How serious is the possible loss of information or intrusion to our HR networks and databases
- How damaging would it be to our business, employees, employees families to lose the data
 - Theft
 - Competitive issues
- Possible breach of contracts if loss is not an act of god or war
- Where would the threats possibly come from
- How would they possibly occur
- When are we exposed, under what conditions
- How long could we sustain interruption with our systems such as
 - Payroll
 - Pension (401K)
 - Visitor access
 - Other vendor needs
- How would we remediate the situation
- How could we recover or replace the data if lost

The risks are then assessed according to the probability of their occurrence, and the damage that would ensue from the loss or interruption. Monetary damages, and replacement costs should be estimated if at all possible, along with the negative publicity and damage to the goodwill of the business, depending on the risk, as sometimes it is not a money issue, but one of the indication of poor management and lack of governance and proper oversight. Each of the risks is then weighed against the others and a prioritized list developed. Cost-benefits trade-offs must be made if the cost on remediation far outweighs the potential loss. The controls and safeguards must be evaluated to ensure they are adequate for the inherent risks.

In addition to HRIT participation, the analysis should include HR, IT, financial, and risk department staff involvement. The assessment should also consider the fact that it is often not a single risk that is the issue, but that several risk events may happen simultaneously.

Plan Development

For the most important risks there should be a plan developed on how to increase the security and safety of the system and/or information that we are concerned with. The plan, like other HRIT projects, should include the estimate of the time and resources, management, and other systems and processes to which changes are needed to deal with the issue. These plans could and should include the possibility of transferring the risk to a third party if competent parties could be found. But using outside and/or off-shore vendors could also increase the risk of moving data and systems to a less than stable business or political environment.

Inherent in this exercise is the fact that there will always be more work that the HRIT and IT groups can handle and these projects must be balanced against other necessary work.

Implementation

Of course if new systems and procedures are required, nothing changes unless a plan is implemented, and as we know the implementation must be handled in a well managed and integrated manner, with all aspects of systems implementation considered. Very often new projects are handled well in the HRIT and IT areas, but change management principles ignored, and some affected employees, parties, users and vendors are not included. In addition, new information access, protection and dissemination policies and procedures may be needed, and the urgency and critical nature of the information should be well communicated.

In any event a total examination of our exposures must be made periodically if we are to stay ahead of the risks we face, and using a template such as the framework will bring about a heightened awareness of the issues and concerns with respect to the HR systems and data for which we are custodians.

A. J. Walker