[**Editor's Note:** The following excerpt is from Chapter 2 of the free eBook *The Definitive Guide to Identity Management* (Realtimepublishers.com) written by Archie Reed and available at http://www.rainbow.com/insights/ebooks.asp.]

Risk and Trust

When evaluating solutions that enforce security, there is always compromise. Within the security space, this compromise is considered risk management. The reason is that generally the more security you put into place, the less usable the system. In line with that consideration is the acceptance that a system has a value to the organization, which must be secured.

Often the only way to calculate the risk is to use a qualified actuarial representative—essentially a statistician who computes risks and premiums, generally for insurance policies. Given that this resource is beyond the reach or reality of most organizations, the calculations are done by internal staff as they attempt to define ROI for a project. Calculating such value is different from organization to organization, and project to project, and can involve basic concepts such as the impact of having employees unable to work overtime due to system security breaches, the potential impact of customers (for example, a boycott), or even legal action against the company. Although calculating the value of more physical considerations is fairly easy, determining the cost of service abuse relative to corporate reputation and similar intangible assets can be very difficult. The point is that as you begin to asses the value of the assets that you are trying to protect, it is important that you utilize representatives from across the organization.

Perhaps a more appropriate baseline to begin assessing risk is to ask more generic questions that can be changed as appropriate for your specific situation, along the following lines:

- How secure is my infrastructure? Is sensitive data protected if disgruntled employees gain access to restricted systems or resources?
- How secure are my connections beyond my infrastructure? Can you ensure that your high-value online transactions are binding?
- How secure are my communications within and external to my infrastructure? Are confidential emails and files protected from interception by unauthorized employees, competitors, and malicious parties?
- Is there a plan to improve security over time?
- Is security actually improving over time?
- Can I transfer risk using different solutions (for example, outsourcing)?
- How does my security compare with that of similar companies in the industry?
- How will I respond to a breach in security?

The important thing to note is that understanding the level of risk you are prepared to accept relates directly to the level of trust you have in your systems and your relationship with other organizations and their systems. This concept of trust becomes very important due to the fine line drawn between fully securing a system such that it is unusable and securing it enough such that risk is mitigated but the system can be used to actually perform the task for which it was implemented.

Beyond this matter, you need to consider impact to your company or “brand”. In the case of any organization, there is risk if untrusted parties with whom you have no legally binding or enforceable agreements gain access to confidential business data, in particular customer or employee data.

The cost of securing a system, let along many systems and their integrated applications, can be astronomical. Consider that the more complex a security solution

- The higher the potential cost of implementation.
- The higher the potential cost of administration and maintenance.
- The more chance that services or data will be unavailable when needed and someone will not be able to do his or her job.
- The more chance that security configuration will be overlooked or someone will not be able to do his or her job.

These truths eventually increase the risks rather than decrease them. This is called the law of diminishing returns.

Identity Management solutions help increase security and minimize the risk of systems by helping manage the lifecycle of a single identity and mapping that identity across multiple systems, principally reducing complexity and cost. A project such as Identity Management that plans to manage information about people and store organizational knowledge will have many security requirements and potential restrictions. As such, you should ensure that your organization has appropriate security policies, and that you are applying the appropriate level of security to the project itself. The optimal scenario for any directory services project is to involve security as part of the core team that will deliver the directory services solution. In this way, you not only gain a representative, or team, who understands the policy and can apply it to the project but also the potential to have the policy changed if there are any issues that are not met, cannot be met, or should not be met. The involvement of security should also be tempered with full interaction with the business representatives to ensure that functionality aspects are not overlooked.

The core nature of Identity Management is to support other networked services and applications. In isolation, an Identity Management solution is useless. As a result, the focus of any security analysis requires a great deal of investigation into the ancillary services to ensure that all potential risks are identified and dealt with in the networked environment.

As we discussed, security is largely about risk management. Once you have assessed your situation, there is a traditional trio of steps to be dealt with when defining and maintaining a security solution that will deal with possible threats to a system. These steps are known as PDR:

1. Protect—In this step, you define your levels of security around the system and the way in which you will implement them.
2. Detect—Despite all the attempts you make to protect a system, there will likely be a way around it, so you need to ensure that you implement monitoring and intrusion-detection into your solution.
3. Respond—To avoid a panic response to a security breach and to successfully deal with breaches of security, you must ensure that there is a step-by-step approach that those involved in the process can easily follow.

These steps define the traditional high-level approach to system security. Within each of the steps are a number of focused activities. To protect a system as well as have any chance of detecting a problem with it, you must understand the system. Seems logical right? Well, unfortunately, many installations of technical solutions are done without considering the aspects of security. It is important that you create a regular review of your environment, especially during times of change.

[**Editor's Note:** This content was excerpted from the free eBook *The Definitive Guide to Identity Management* (Realtimepublishers.com) written by Archie Reed and available at http://www.rainbow.com/insights/ebooks.asp.]