

Information Risk Management: Why Now?

Christian Byrnes byrnes@centraxcorp.com
CEO, Centrax Corporation

Information Risk Management: Another thing to invest limited budget and time into in the name of security. Why me? Why now? In fact, a successful enterprise security plan balances appropriate (and selective) enforcement techniques with broad-based Information Risk management capabilities, both of which are based on and prioritized via well-designed security policies.

The long-term objective of security is to become transparent. All approved access to computing resources should happen without the user being aware that a security mechanism exists. All improper access should be denied. The unsatisfied worldwide demand for "single sign-on" is one of the ways this objective is expressed. While we wait for this nirvana-like state to become achievable (analysts estimate 5+ years), security needs must be met through other means. Indeed, even if we could build such an ideally secure computing infrastructure, we will continue redefining (and monitoring) appropriate behavior to meet new business needs.

Access to applications and information drives technology implementation. The security functions of technology constrain access so that only actions that are appropriate can take place. If the technology is perfect, and if we can fully understand what behaviors are appropriate, then security is easy. Oops. In fact, complete security is impossible. Even worse, reasonable security may severely impact appropriate access, thus undermining the business decision to use computer technology in the first place. But when it is done right, security improves our ability to do business. Here is how to approach enterprise security the right way.

The Whole Security Space

Achieving reasonable levels of security with minimal impact on business operations requires evaluation and use of a wide variety of tools and techniques. Each of those can be categorized as either enforcement or Information Risk Management. Both categories can be further broken down into perimeter or internal.

Table 1 shows the most significant enforcement areas and the typical approaches used for perimeter and internal security.

Table 1.

	Enforcement Approach	
	Perimeter	Internal

Access Control	Firewall and proxy server	Operating system facilities
Authentication	Remote access devices	Single sign-on attempts
Authorization	Filtering routers	Application logic or RDBMS
Identification	Tokens	Password policy

Clearly, perimeter enforcement is significantly more mature than internal enforcement. There are two reasons for this. First, the cost of enforcement is high. An identification token frequently costs \$75 plus the investments in integration, support and lost productivity when security interferes with business (for example, lost cards, broken cards, improperly denied access). Therefore, identification tokens are issued only to remote workers; never to all internal employees.

The second reason that perimeter enforcement is more mature than internal security approaches is that the threat posed by outsiders has been considered to be higher than the threat from insiders. Given the costs per user and the limited staff resources available to most security organizations, perimeter defenses came first.

Table 2 shows the most significant Information Risk Management areas and the typical approaches used for perimeter and internal security. More detail on the implementation, features, and use of Information Risk Management tools can be found in the September 1998 issue of *Windows NT Systems*.

Table 2.

	Information Risk Management	
	Perimeter	Internal
Security Posture/Assessment	SATAN-type scanners	Agent technology
Policy and Configuration Management	Firewall consoles	Agent technology
Intrusion Detection	Packet sniffer analyzers	Log analyzers
Damage Assessment	Not possible	Log analyzers

Perimeter tools for Information Risk Management have been largely derived through

commercialization of freeware tools. While this has enabled many vendors to rush products to market, those tools have proven to be risky in their execution and difficult to manage.

Internal tools for Information Risk Management, while relatively new to the market, do not have the same weaknesses as internal enforcement tools. The cost of perimeter and internal Information Risk Management tools are approximately equal. Integration and management costs for them are much lower than for any class of enforcement tool.

In addition, the protection provided by internal tools in this area includes virtually all of the outsider threats, thus reducing (but not eliminating) the need for the riskier perimeter tools.

Protecting Assets and Achieving Piece of Mind

If we accept that security is not absolute given the current technology available to us, then we must face some level of uncertainty about the current state of protection that we are providing for corporate (or agency) assets. Not even over-investment in enforcement tools can provide us with sufficient protection to state that we have done enough.

A good example of this problem is the security state of Microsoft's NT Server operating system. It passed US government tests for level C2 security. This represents a significant achievement, and demonstrates that NT can be secure. But the trade press has been hounding Microsoft for the last year with reports of various security breaches. Is NT secure or not?

The answer is that NT, like every other operating system, can be made reasonably secure. Just as in the UNIX environment, a good system administrator, working closely with the operating system vendor, can meet reasonable demands for security. No computer is perfectly secure. When all reasonable precautions have been taken and the security configuration tools of the operating system (or third party vendors) have been properly applied, then the resulting environment *must* be monitored for unexpected or inappropriate activity. This is the only means of determining that sufficient safeguards have been implemented, that no back doors have been left in the system and that the security configuration has remained in its intended state.

Most security conscious organizations provide some attempt at Information Risk Management through the operational audit process. External and internal audit processes are independent of both the security organization and IS. Operational audit, in contrast, is performed by the security organization as a routine part of ensuring security. Typically, audit policies are defined and implemented when systems are installed and are kept common across all servers. The audit logs produced are centralized and reviewed by junior members of the security staff; frequently on a spot check basis. Given sufficient skilled staff, this approach can provide a significant level of surety that due diligence has been exercised in providing security for the enterprise. Information Risk Management tools automate this process, reducing its cost, reducing the skill requirement, and dramatically improving its effectiveness.

The Successful Sequence

With four enforcement types available for internal and perimeter protection, and four Information Risk Management functions also needed for both internal and perimeter protection,

some sense is needed of prioritization and sequence. Clearly, establishing enterprise security is not a small project. All security decisions should be governed by policies. Therefore, the first step must be to create the security policies. Security policies codify the enterprises' willingness to invest in and accept the limitations imposed by security. A single short document sits at the top of the policy hierarchy. This is sometimes referred to as the security charter.

Step two in establishing enterprise security is designing security domains. These may or may not coincide with any of the existing domain designs (for example, NT resource or user domains). Security policies are then assigned to the domains. Resource classification schemes (unclassified, secret, top secret, and so on) can be very useful during this step.

Step three is to assess the current security posture and evaluate risk. This step provides the information needed to select from the list of enforcement and Information Risk Management techniques and to prioritize implementation. Of course, the assessment can be assisted by appropriate Information Risk Management tools. Both the assessment and the risk analyses must be done relative to the security policies defined in step one.

Step four is to select and implement solutions. High-value, high-risk, server-based resources should be protected with strong enforcement technologies. Those imperfect technologies should then be monitored with Information Risk Management tools. Security domains that hold only moderate risk and/or moderate value resources may not justify an extensive investment in enforcement mechanisms. Frequent assessments and constant monitoring will be sufficient to meet normal business security needs and will have no impact on business processes.

A successful enterprise security implementation is a win/win investment. Management and staff can rest better knowing that the threat to valuable resources has been significantly reduced and that valuable business data will be available, uncontaminated and still, secret when they return to the office in the morning. Executive management (and the Board of Directors) can be assured that meaningful and appropriate measures have been taken to protect the interests of investors. Done well, security is a win.

* * *

Christian Byrnes is the chief executive officer of Centrax Corporation. He is widely recognized as one of the top industry analysts for information security during his four years at the META Group. His book in Security in Enterprise Computing: A Practical Guide was published by META Group. Mr. Byrnes can be reached at (619) 546-2400 or at byrnes@centraxcorp.com.