Security Management

By Joe Feliu in conjunction with Harris Kern's Enterprise Computing Institute

Description: Security is a huge topic and presents a host of challenges to the CIO. As you feel confident that one security vulnerability is addressed, another one arises. This state of affairs will not change in the foreseeable future. So, what is the CIO to do? There are five management steps that each CIO should be taking to minimize risk.

1. Appoint a Security Officer or Security Committee. Depending on the culture and size of your organization, establish a single point of accountability for all information security matters.
2. Establish and communicate an Information Security Policy. It is imperative that the information security position of the company be documented and communicated throughout the company for practical and legal purposes.
3. Conduct a security risk assessment to assess the current state of security readiness. Identify key vulnerabilities and develop a plan of action to address each.
4. Implement standard security processes, procedures and tools including:
    - Intrusion Detection Systems
    - Firewalls
    - Robust backup and recovery systems and processes
    - Update applications and operating systems with latest security patches
    - Trained security technicians
    - Access authentication – use strong password access to all information, systems and facilities (smartcards, public key infrastructure and biometrics where needed)
    - Encryption
    - Virtual Private Networks
    - Antivirus software
    - Periodic security audits
5. Champion an organization-wide security awareness training program. Remember, the weakest link in most systems is the human factor. Bruce Sneier states it so well in his book Secrets and Lies – Digital Security in a Networked World, "Social engineering bypasses cryptography, computer security, network security, and everything else technological. It goes straight to the weakest link in any security system: the poor human being trying to get his job done, and wanting to help out if he can."

Benefits: Protecting the security of the information assets of the company is a core responsibility of the CIO. The fundamental principles of asset protection apply, and often the CIO is the cornerstone for the protection of the critical intellectual property of the company. As with any other technology responsibility, there are issues of cost justification. However, those of us who have experienced major breeches in security know full well how costly a "security event" can be. Make security one of your top priorities.

First Steps: Begin your new emphasis on security using the following steps:

1. Appoint a Security Officer or Security Committee
2. Develop and publish an Information Security Policy

3. Launch an abbreviated risk assessment initiative and take corrective actions on key vulnerabilities

Example: A sample template for a server security audit is presented in Figure 1 below.

SERVER SECURITY AUDIT

System Name/Type/Administrator: Although the primary unit for this assessment is a server, some system classes such as desktops and HR security are not server specific. The Systems Name, Type (e.g. Novell, NT, Unix, etc.) and Systems Administrator must be included for each server. A class of servers may be included on one form; in this case, place the name, type, and systems administrator for all servers in these sections.

System Class/Audit Area details the specific item to be audited or commented on.

Level indicates relative importance of item.

A = Business Critical – Must be complied with for legal or other business reasons. If not 100% compliant, explain in comments with expected compliance date.

B = Region or Business unit may make determination of critical nature. If compliance is needed, explain in comment area with expected completion date.

C =Compliance is advised, but not required. Comment as necessary.

Compliance - indicator of percentage of compliance of each item that is currently in place. To the degree possible, objective and verifiable measures s be used to determine compliance level.

Comments - include any explanatory comments as desired.

Note: for all Level A items for which there is not 100% compliance, include the date when 100% compliance will be achieved.

Location: Headquarters	**Assessed by: Jane Doe**		**Date: 6/12/2003**
System Name: SAP			
System Type: Unix Systems			
System Administrator: John Smith			

	System Class/ Audit Area	**Level**	**Compliance**	**Comments**
1.	**Servers – Physical Security**			
1.1.	All servers are maintained in a physically secured location	A	100%	
1.2.	Access to server location monitored and logged	B	100%	
1.3.	HVAC is adequate for all servers and systems at location	A	100%	
1.4.	UPS for all critical systems	A	100%	
1.5.	Fire suppression systems adequate for server location	A	100%	Upgrade scheduled-9/03
2.	**Servers – Logical Security**			
2.1.	Procedures documented and implemented to manage Supervisor Accounts	A	100%	
2.2.	Procedures documented and implemented to manage concurrent user connections	C	100%	
2.3.	Procedures documented and implemented to ensure user passwords are unique, of a minimum length, and are required to be changed periodically	B	50%	Procedures in final review; will be implemented by 10/03
2.4.	Server console access is restricted	A	100%	
2.5.	System login auditing is enabled and audited	B	100%	
2.6.	The number of invalid log-on attempts are limited	B	100%	
2.7.	Inactive users are logged out after a specified period of time	C	0%	To be completed-10/03
3.	**Desktops/Workstations – Physical Security**			
3.1.	Procedures documented and implemented to secure the hard drive of portable computers	B	100%	
3.2.	Procedures documented and implemented to recover data from terminated employee systems	B	100%	
3.3.	Cable-security device provided for all portables	B	30%	To be completed-12/03
3.4.	Intrusion detection seals provided on all workstation case housings	C	100%	
4.	**Desktops/Workstations – Logical Security**			
4.1.	Power on password initiated for all portables	B	100%	
4.2.	Screen-saver passwords enabled on workstations	B	100%	
4.3.	Individual logins required on networked workstations	C	100%	
5.	**Data – Physical Security**			
5.1.	Redundant physical drives for all critical data file systems	A	100%	
5.2.	Procedures documented and implemented to verify drive physical integrity	B	100%	
6.	**Data – Logical Security**			
6.1.	Procedures documented and implemented to ensure encrypting of sensitive data	B	100%	
6.2.	Procedures documented and implemented to ensure integrity of locally stored data (e.g. server backup)	A	100%	
6.3.	Procedures documented and implemented to ensure latest release of anti virus software is running in real time on all servers	A	80%	To be completed-8/03
6.4.	Procedures documented and implemented to ensure all desktops are running anti-virus software	B	100%	

7.	**Peripherals – Physical Security**			
7.1	Paper shredder facility available near printers	B	100%	Consolidated shredding station on each floor
7.2	Printer output stored in labeled bins	C	100%	
7.3	Scanners monitored for appropriate use	C	100%	
7.4	Digital cameras monitored for appropriate use	C	100%	
8.	**Peripherals – Logical Security**			
8.1	Peripheral use logged where appropriate	B	100%	Computer room only
9.	**Remote Access – Physical Security**			
9.1	All modem's are accounted for at all times	A	100%	
9.2	All data-capable communication lines are secured and routed through a common location for monitoring	A	100%	
10.	**Remote Access – Logical Security**			
10.1	Procedures documented and implemented to ensure dial-in access is secure	A	100%	
10.2	Dial-in access is limited to specific job functions, with access levels tied to function	B	100%	
10.3	Remote access sessions are logged	A	60%	To be completed 8/03
10.4	Procedures documented and implemented to detect remote control software accessing network servers	B	100%	
10.5	Desktop modems have dial-out access only, or connected only when in use	B	100%	
10.6	Desktop and centralized FAX (outgoing and incoming) access is logged	B	100%	
11.	**Infrastructure – Physical Security**			
11.1	Infrastructure components are physically secure from intruders, both deliberate and accidental	B	100%	
11.2	Building entrance devices (demark) are locked and checked	A	100%	
11.3	Procedures are developed and implemented to verify physical security of infrastructure	B	100%	
12.	**Infrastructure – Logical Security**			
12.1	Logical maps of devices are maintained	B	100%	Update bi-annually
12.2	Procedures have been documented and implemented to check for logical intrusions (scanners)	A	100%	
12.3	Sensitive material and passwords are encrypted on-the-wire	B	100%	
13.	**Human Resources Issues**			
13.1	Computer security policies have been developed and published	A	30%	To be published – 12/03
13.2	Computer Security training plan has been developed and implemented	B	100%	
13.3	Password policies have been implemented and are audited	B	100%	

Figure 1 – Server Security Audit

==========

The Enterprise Computing Institute (www.ecinst.com) helps IT professionals solve problems and simplify the management of IT through consulting and training based on the best-selling Enterprise Computing Institute book series. Founded by Harris Kern (www.harriskern.com), the industry's foremost expert on simplifying IT and world-renowned American author, publisher, lecturer, and consultant, the Institute has focused on providing practical guidance for tackling current IT challenges since its inception in 1998.