

Libraries, Computing & Technology

Computer and Network Security: Questions Everyone Should Ask

*A guide for discussion among business
administrators and their information
technology staff*



MICHIGAN STATE
UNIVERSITY

Computer and Network Security: Questions Everyone Should Ask

A guide for discussion among business administrators and their information technology staff

Overview

Today virtually every business function at the university involves use of information technology. We use computers to store and retrieve records and we conduct online transactions over building, campus and Internet network connections.

Information technology yields great efficiencies and analytical power; it also imposes the responsibility to manage information securely and in many cases confidentially.

This report provides a checklist to use in evaluating whether a unit is adhering to best practices in computer security and data confidentiality.

Security experts advise that *computer security is an ongoing process, not a single safeguard or product*. Rather, *computer security is achieved through an ongoing process of assessing risks, managing risks, and monitoring the effectiveness of risk mitigation techniques*.

In today's world security requires constant vigilance.

Scope of this Document

This document provides a guide for discussions among computer support staff and management. Computer security is a complex subject area to which many books and journal articles have been devoted. Computer security also involves the processes used to plan, acquire, and implement technology, as well as the management processes for authorizing and approving business transactions. Therefore this document cannot be considered comprehensive. Instead, it is a starting point for discussion. Consult the computer security resources listed at the end of this document for more information.

Most of this document is presented in question format. These questions imply security practices that units should consider implementing; however, some of this material may not apply to a particular department or operating environment.

Securing New Systems

- When we acquire a new server or desktop computer, do we follow a defined set of procedures to set it up?
- How do we “lock down” a new system? Do we:
 - Turn on or install software firewalls?
 - And/or use a hardware firewall?
 - Turn off unnecessary services (e.g. FTP on a desktop computer that doesn’t need to support this protocol)?
 - Rename administrator user names as appropriate? Change default passwords?
 - Follow product-specific advice or expert checklists on how to secure new servers and applications? *(For instance, software vendors and outside experts offer white papers or checklists on how to secure, for instance, a Windows XP workstation or a Linux server.)*
- Do we test new systems for security using tools such as the Microsoft Baseline Security Analyzer, etc?

Password Management

- Who knows the passwords for systems that perform critical business functions?

- Do we regularly change passwords on critical systems?
- Do we require end users to change their passwords? How often?
- Do we educate end users about good password choices? (e.g. avoid family names and dates, use a password longer than 6 characters, don't use words found in dictionaries, include numerals in the password).
- Do we discourage sharing of user names and passwords among multiple people?
- Do we provide tools to help people choose strong passwords? (Note: some system administrators use automated tools to scan the user database or password file for easily-guessed passwords.)
- Do our systems "lock out" an account after a pre-determined number of failed login attempts?
- How do we manage which people have privileged access to our systems? Do we periodically review which people have "root" or "superuser" or "administrative" privileges on systems? Do we have a procedure to remove privileges for employees who have left the university? Do we remove privileged access when an employee no longer needs it?
- Do we ensure that in case of emergency someone will have passwords for critical systems (for instance, if the primary system administrator is unavailable).

Anti-Virus

- Do we run anti-virus software? Which tool(s) do we use?
 - On all servers? On all critical desktops?
 - On all end user desktops?
- Are our virus definitions current?
 - How often are the definitions updated? (At least twice weekly is advised; many experts suggest daily updates.)
- Do we run spyware detection software on our servers and on end user computers?

- How are servers and end-user computers given new antivirus definitions? (From the vendor's Web site, from a local server, or otherwise?)
- Have we enabled automatic scanning for virus definition updates on servers and end-user computers?
- Do we scan incoming and outgoing email for viruses (as well as other modes of transmission)?
- Do we educate our users about virus avoidance (e.g. be wary of attachments in general, don't run .EXE files sent via email, etc.)
- Have we considered limiting the ability of end-user computers to install new software, so as to limit the capacity of viruses to install themselves?
 - E.g. using Microsoft's Group Policy Option?

Software Maintenance

- How often do we apply vendor updates operating system software? Office productivity software? Other software?
- When we update computers, do you have to physically visit each computer, or do you use centralized management tools (e.g. SUS for Windows)?
- Do we set up computers for automated scheduled software updates?
- Suppose that major media are reporting that Microsoft has released a patch to close a major vulnerability in Windows. We need to update all our Windows computers immediately.
 - How would we rapidly communicate with all users in the department?
 - How long will it take us to complete this task for the 100 computers in our department?
 - What about patching laptop computers our users have off-site?



- Should our users power down their computers or unplug them from the network until we can do this update?
- Do we allow end users to install operating system patches (e.g. Windows Update)? Do we allow end users to install applications software?

Backups

- How often do we back up our servers? How often do we back up the desktop computers that we use for departmental business functions?
 - A common practice is weekly backups of all data, and daily backups of files or data that have changed.
- What backup media do we use? Is hardware to read that media commonly available?
- When did we last test our backup procedures to make sure data can be restored?
- Are our backups in “image” format (requiring identical hardware or software to restore)? Could we load our backups into another system if need be?
- Do we take backup tapes offsite? Where? How often?
- How often do we back up end user desktops? Or is this the responsibility of end users?
 - Example: Professor I. M. Scholarly comes into my office and says a water pipe just ruined his computer and 10 years of research is lost. Do we have a backup copy of his data? How old is the backup? Was it backed up remotely from his computer?

Physical Security

- Are all of our servers and critical desktop computers kept in secure areas?
 - Who has keys (traditional, key-card, or both) to the doors for those areas?

- Do we periodically review access lists and remove access for those people who no longer need it?
- Are areas that house critical systems protected by alarm systems? Should they be? (Note: the university has mandated that installation of any alarm systems on campus must be coordinated with DPPS.)
- How are backup tapes/discs secured in transportation and in storage
- Who has access to backup tapes we take offsite?

Network Security

- Do we use hardware firewalls to protect critical servers and desktop computers?
 - How often do we examine event logs and real-time displays to see if we are under attack?
 - Do we use software firewalls to protect end-user computers (e.g. laptops that may spend time away from protection of the departmental hardware firewall)?
- Do we monitor the network for security exposures using auditing tools such as ISS, or Nessus?
- Do we monitor the network for unusual patterns of traffic? (e.g. an end user desktop suddenly begins emitting huge amounts of traffic).
- Do we ensure that all critical business transactions take place using encrypted transmission? (E.g. SSL for Web or email transactions, SSH or VPN for remote login, encrypted file transfers)?

Wireless Security

- Have we educated our users about the risks of using wireless (Wi-Fi) networks, especially on unsecured open networks (e.g. public spaces such as at many hotels and coffee shops)?
- Do we encourage use of encryption above network layer such as SLL or Virtual Private Networks (VPN)?
- Do we operate Wi-Fi access points in our unit? If so:
 - Have we turned off the broadcasting of SSIDs?

- Do we require an encryption key (WEP or WPA) to use our access points?
 - How do we manage the passphrase?
 - Do we enforce periodic changes to passphrase?
- Whom do we let connect to our access point(s)
 - Just people in our department? Guests? Anyone?
- How do we monitor activity over our wireless access points?

Data Security

- What confidential personal information (e.g., Social Security numbers) do we store on our servers? Do we minimize use of SSNs to the extent feasible? Could we use another identifier, such as MSU PID numbers instead?
 - If we *do* need to store confidential data such as SSNs locally, how secure are the servers that house the information?
- Instead of storing personal confidential information locally, could we do business in some other way? Could we eliminate those confidential data elements from our local databases? Could we instead routinely access data as needed from University data services (thus obviating the need for the local copies)?
- Have all personnel within the unit been adequately trained in University data security requirements and applicable state or federal laws and regulations (e.g. FERPA, HIPAA, Gramm-Leach-Bliley Act)?

Intrusion Detection and Recovery

- Assume this scenario: *The network security staff at the Computer Center just informed me that a computer in our department is infected with the ReallyBig virus. It is disrupting network performance, sending out thousands of infected emails, and serving first run movies to pirate worldwide.*
 - What do we do immediately? Would we remove the compromised system from the network?
 - What sort of investigation would we carry out to determine the nature of the attack, and what vulnerability was exploited, and what data may have been compromised?
 - How would you restore this computer to normal operation?

- Do you intend to disinfect it, or format the hard drive and reinstall operating system and software (perhaps from “ghost” image)?
- Do we regularly monitor event logs on servers, other computers, and firewalls to look for patterns of attack? Are the logs available after an attack?

Disaster Recovery Planning

- Do we have a written disaster recovery plan?
 - Are copies in possession of departmental management? At their homes?
- When was our plan last updated?
- Does our plan include:
 - A list of who in the department is empowered to declare a disaster? A list of critical personnel who will need to respond to a disaster?
 - Telephone numbers (home, cell) for all critical personnel?
 - An inventory of all our critical business functions?
 - An inventory of the computer systems that support those functions?
 - Including not only servers but critical desktop computers (e.g. departmental secretaries’ computers)?
 - A rank-ordered list of which business functions we would restore first in event of a disaster?
- Suppose we had to evacuate the building due to a major disaster (fire, flood, chemical or biological event renders building inaccessible). Suppose all our systems are offline. How long would it take to restore basic departmental business functions and data from our offsite backup tapes?

Current Awareness of Security Issues

- What news sources do you use to stay abreast of new security risks? Resources include:

- Security-related Mailing lists
- CERT Coordination Center: <http://www.cert.org/>
- Alerts from major software vendors
 - Major software vendors (e.g. Microsoft, Apple, Adobe, Corel)
 - Vendors of anti-virus software (e.g. Symantec, Trend Micro, McAfee)
- News media alerts (*Major media often cover virus outbreaks and other security issues. A news aggregator such as Google News can help you search for breaking news, for instance about a new virus outbreak.*)

Computer Security Resources

MSU Resources:

- Security.msu.edu
- MSUSEC mailing list
- MSUNAG mailing list

Other Web Sites

- Educause's "Effective Security Practices Guide: Balancing the Need for Security and Open, Collaborative Networking" *This Web site offers an overview of IT security strategy as well as specific white papers detailing best practices from IT divisions of major leading universities.* <http://www.educause.edu/security/guide/>
- National Security Agency Security Configuration Guide. *A collection of guidebooks with step-by-step procedures for securing various versions of operating systems, database package, applications software, and network equipment.* <http://www.nsa.gov/snac/>

Books

Numerous books cover the area of computer security. Please consult the MSU Libraries or other library or online resources for relevant titles.