Cyber-Security Audits & Policies

Dr. Paul Lynch - Lynbrook
Dan Friedman - Hicksville

Area #1 – IT Policy

Computer policies define appropriate user behavior, describe the tools and procedures needed to protect data and information systems, and explain the consequences of policy violations.

The governing board should provide important oversight and leadership by establishing computer policies that take into account people, processes and technology; communicating the policies throughout the organization and ensuring there are procedures in place to monitor compliance with policies.

Recommended Policies

- Breach Notification Policy - 8635
- Internet, Email, and Personal Computer Use - 4526
- Use of and Access to Personal, Private, and Sensitive Information - PDBoR
- Password Security- 4526 and 4526.1
- Wireless Security Policy - 4526E
- Mobile Computing and Storage Device Policy - 8340
- Online Banking - 6635 or 6430

Area #2 – IT Security Training and Awareness

A well-informed work force is the strongest link in the chain to secure electronic data and computer systems. Entities cannot protect the confidentiality, integrity and availability of their data and systems without ensuring that the people who use and manage IT understand organizational IT security policies and procedures and their roles and responsibilities related to IT security. While the IT policies tell computer users what to do, cybersecurity training provides them with the skills to do it.

Area #3 – Computer Hardware, Software, and Data Inventories

Organizations should maintain detailed, up-to-date inventory records for all computer hardware, software and data. The information maintained for each piece of computer equipment should include a description of the item including the make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase or lease information including the acquisition date.

Software inventory records should include a description of the item including the version and serial number, a description of the computer(s) on which the software is installed and any pertinent licensing information.

Area #4 – Contracts for IT Services

Local governments and school districts increasingly rely on third parties to provide a variety of IT-related services. For your protection and to avoid potential misunderstandings, there should be a written agreement between your organization and the IT service provider that clearly states your organizational needs and expectations including those relating to the confidentiality and protection of personal, private and sensitive data and specify the level of service to be provided by the vendor.

Area #5 – Virus Protection

Malicious software, or malware, are software programs that are designed to harm computer systems. These programs can wreak havoc on both systems and electronic data by, for example, deleting files, gathering sensitive information such as passwords without the computer user's knowledge and making systems inoperable.

Area #6 – Patch Management

A “patch” is software that is used to correct a problem, such as a security vulnerability, that exists within an application or an operating system. Security vulnerabilities in software can be exploited to infect a computer with a virus, spyware or other malicious agents or to gain access privileges illicitly. When security vulnerabilities in software are discovered, the software vendor typically issues a free patch (fix) to correct the problem.

Area #7 – Access Controls

Computer access controls prescribe who or what computer process may have access to a specific computer resource, such as a particular software program or database. For example, access controls can be implemented to limit who can view electronic files containing employee names and Social Security numbers. The first step in implementing adequate access controls is determining what level and type of protection is appropriate for various resources (e.g., data) and who needs access to these resources.

There should be written procedures in place for granting, changing and terminating access rights to the overall networked computer system and to specific software applications. These procedures should establish who has the authority to grant or change access (e.g., department manager approval) and allow users to access only what is necessary to complete their job duties.

Area #7 – Access Controls - Passwords

Complexity Requirements–A complex password should contain at least one uppercase character, one lowercase character, one numeric character and one special character (e.g., %, #, @) and not include names or words that can be easily guessed or identified using a password-cracking mechanism or dictionary. Furthermore, the password should not contain any part of the account, network or municipality names.

Length–Passwords should be sufficiently long; that is, at least eight characters in length. Passwords longer than eight characters may provide greater security, but those benefits could be offset by people having to write down the password in order to remember it.

Aging–Passwords should be changed periodically, about every 30 to 90 days. The more sensitive the system or data involved, the more frequently passwords should be changed.

Reuse of Old Passwords–Organizations should consider placing limitations on the reuse of old passwords.

Failed Log-On Attempts–To prevent password guessing and online password attacks, failed log-on attempts should be limited to three to seven consecutive attempts.

Area #8 – Online Banking

Despite online banking establishments' security controls, there is no way to absolutely guarantee the safety of online banking. The tactics used to commit fraud can range dramatically in sophistication and continually evolve over time. Likewise, there is no single control that is most effective against cyberattacks. A best practice for protecting IT systems and information is to build successive layers of defense mechanisms, a strategy referred to as defense-in-depth, a concept discussed earlier in this document.

Area #9 – Wireless Network

Wireless networks are exposed to many of the same types of threats and vulnerabilities as wired networks, including viruses, malware, unauthorized access and loss of data. However, they are considered inherently less secure than wired networks because their information-bearing signals are broadcast or transmitted into the air. These traveling signals potentially can be intercepted and exploited by individuals with malicious intent. Since wireless networks are used as extensions of wired networks, even minor flaws in the configuration and implementation of a wireless segment can impact the security of an entire network. A wireless environment, therefore, requires certain additional security precautions.

Area #10 – Firewalls and Intrusion Detection

Networks that are connected to the Internet are physically connected to unknown networks and their users all over the world. While such connections are often useful, they also increase the vulnerability of computerized information to access and attack from unauthorized individuals. Firewalls consist of hardware and/or software that enforce boundaries between computer systems and the Internet. Firewalls control network traffic flows, using rule sets which specify which services will pass through the firewall and which services are kept out. Firewalls can also act as effective tracking tools and can perform important logging and auditing functions. For these reasons, the network administrator should log and periodically review firewall activities/events.

Area #11 – Physical Controls

Physical security controls restrict physical access to computer resources and protect these resources from intentional or unintentional harm, loss or impairment. Such controls include guards, gates and locks, and also environmental controls such as smoke detectors, fire alarms and extinguishers, protection from water damage and uninterruptible power supplies.

Area #12 – Information Technology Contingency Planning

The impact of an unplanned IT disruption involving the corruption or loss of data or other computer resources from human error, malware or hardware failure, could significantly curtail an organization's operations. Proactively anticipating and planning for such IT disruptions will prepare local government and school district personnel for the actions they must take in the event of an incident.

Additional Resources

Center for Internet Security
https://www.cisecurity.org/

Industrial Control Systems Cyber Emergency Response Team
https://ics-cert.us-cert.gov/

National Institute of Standards and Technology
http://www.nist.gov/

New York State Office of Information Technology Services
https://www.its.ny.gov/

New York State Office of the State Comptroller
http://www.osc.state.ny.us/

United States Computer Emergency Readiness Team
https://www.us-cert.gov/