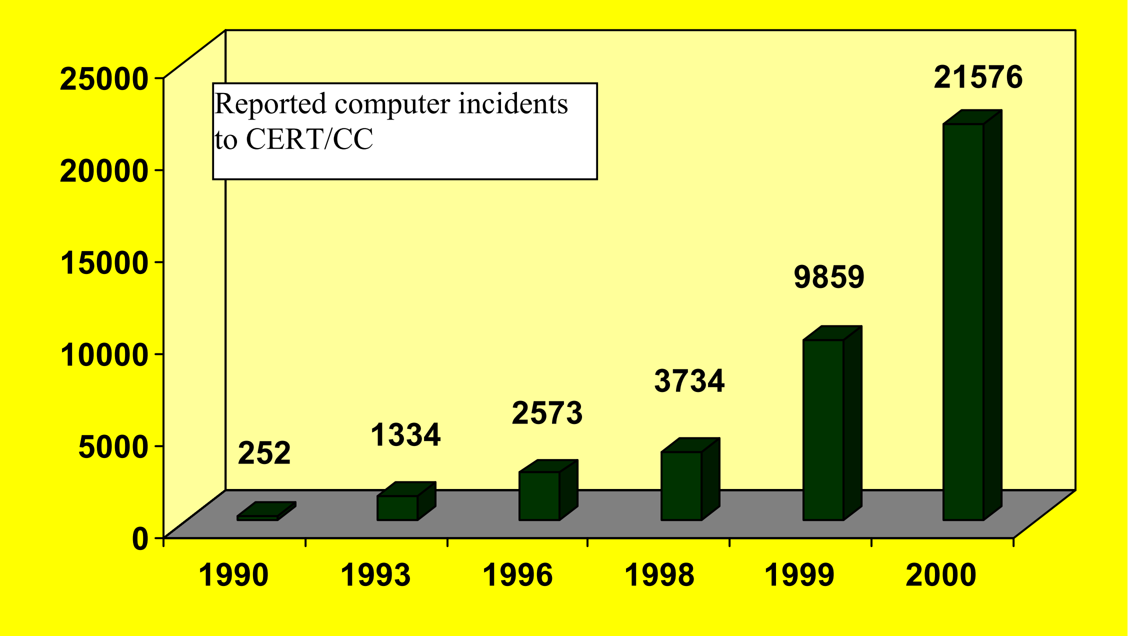
Information Systems - Network Security Guidelines

Rapidly evolving technologies continue to provide efficient, cost effective methods for providing fast delivery of a wide range of member services. Accompanying the opportunities to deliver cost effective services is growing exposure of technology resources to misuse and theft, which can result in loss of member confidence. Intrusion and abuse of technology is growing at an escalating rate. Intrusions, as noted in the chart below, reflect an increasing average rate of approximately 300 percent annually. The data was provided by Computer Emergency Response Team/Coordinating Committee (CERT/CC).



The CERT/CC[1] is a government sponsored organization operated by the Carnegie Mellon Software Engineering Institute. Part of its mission is to track vulnerabilities in computer systems and recommend methods to improve computer security. Incidents are voluntarily reported and include:

1. Attempts to gain unauthorized access to a system or its data;
2. Unwanted disruption or denial of service;
3. Unauthorized use of a system for the processing or storage of data; and
4. Changes to system hardware, firmware, or software without the owners' knowledge, instruction, or consent.

In addition to their disruptive nature and erosive effect on customer confidence, intrusions and system weaknesses are causing significant financial losses. In a recent survey conducted by the Computer

[1] For additional information and resources on CERT the Website is www.cert.org

Security Institute[2], 273 organizations reported $265,589,940 in financial losses. Sixty-seven percent reported serious criminal actions that include theft of proprietary information, financial fraud, system penetration from outsiders, denial of service attacks, and sabotage of data or network. The most serious categories of loss were theft of proprietary information ($66,708,00) and financial fraud ($55,996,000). The Institute reported the year 2000 was substantially higher than any other year in the survey's five-year history.

The survey data adds a financial perspective to the continual news of penetrations and disruptions of large corporations and major Internet service providers. While major news events cover disruptions at the larger sites, the data strongly suggests losses are occurring on a regular and escalating basis at all business levels. The guidelines presented here constitute the benchmarks utilized in OCCU's supervision program of corporate information system (IS) activities.

Guidelines for Corporate Information Systems Security - An effective oversight program should involve active participation of all staff and departments. The basic elements of any program should consist of developing a security policy, performing vulnerability assessments, establishing a network-monitoring program, and performing periodic penetration testing.

1. **IS Security Policy** - The focus of a security policy[3] is a strategy for protecting corporate assets. It should reflect management's commitments, employees' obligations, and form a framework for implementing secure practices throughout the organization. Critical elements include:

    a. Appointing a corporate security officer who is responsible for implementing the program.
    b. Identifying critical information system assets together with who has responsibility for ensuring their security.
    c. Specifying processes and procedures for protection of the assets.
    d. Developing an ongoing employee-training program in computer security.
    e. Formulating a corporate firewall policy that addresses who and what services will be permitted into and out of the corporate network.
    f. Appointing a computer emergency response team. That team would focus on responding to security alerts and intrusion attempts.

2. **Vulnerability Assessments** - Implementing a security policy begins with a vulnerability assessment of the corporates' technology base. The scope of a vulnerability study includes network infrastructure, user authentication procedures, and organizational security practices. This work is usually accomplished by a combination of staff resources, outside consultants, and automated network analysis tools. A thorough vulnerability assessment will provide corporate management with the information needed to identify the greatest risks in the information

[2] The survey was conducted with the participation of the San Francisco Bureau of Investigation's Computer Intrusion Squad. Background information and a summary of the study is available at www.Gocsi.com. Another recent document pertaining to internet service providers is "Recommended Internet Service Provider Security Services and Procedures". It is Request for Comment (RFC) 3013 at www.RFC-editor.org.

[3] RFC 2196 discusses, in detail, considerations needed in a security policy. The RFC can be obtained at www.RFC-editor.org. A more concise summary of security policy development is outlined in "An Introduction to the OCTAVE Method" at www.cert.org.

technology environment. Once the majority of risks identified in the study are addressed, a continuing program of vulnerability assessments should be established to ensure that newly evolving network weaknesses resulting from configuration changes, routine maintenance, and implementing new systems are quickly identified and resolved.

3. **Network Oversight Program** - This process is driven by the corporate security policy and includes correction of vulnerabilities noted in the network security assessment. Vigilance and continual refinement of the corporate security infrastructure are the primary lines of defense to safeguard corporate technology. An oversight process should involve the efforts of IS staff, internal/external auditors, IS service providers, and the corporate security officer or committee.

    a. IS Staff
        1. Takes maximum action to remove system vulnerabilities by applying program fixes, service patches, and upgrades on an ongoing basis;
        2. Removes all unnecessary services from network servers;
        3. Ensures corporate firewalls conform with security policy;
        4. Benchmarks critical servers to comply with corporate security policy; and
        5. Reviews all event logs and system activity for possible intrusion attempts and unauthorized file access.

    b. Internal Audit
        1. Monitors compliance with the corporate security policy;
        2. Reviews vulnerability scans to documents patches, upgrades, and system benchmarks;
        3. Monitors employee use and access permissions to ensure appropriate use;
        4. Reviews administrative activity logs for appropriate use and compliance with corporate policy; and
        5. Monitors firewall benchmarks and related change control processes.

    c. Third Party IS Providers
        1. Provide adequate documentation that their networks and services are provided in a secure environment; and
        2. Update software regularly to ensure system security.

    d. Corporate Security Officer
        1. Ensures employees are adequately trained in network access procedures, file control, and password enforcement;
        2. Oversees compliance and implementation of corporate security policies and procedures. Outside assistance is utilized as needed;
        3. Revises the security policy as needed to stay current with technology risk; and
        4. Reacts promptly to intrusion attempts and other improper use of corporate information systems resources.

The implementation process usually requires automated tools in all but the smallest network environments. There are a wide variety of event log monitoring tools, vulnerability scanners, and intrusion detection systems that will assist in the oversight process. Given the escalating number of vulnerabilities, intrusion attempts, and documented losses, an effective oversight process will require adequate resources to ensure protection of critical corporate assets.

4. **Penetration Testing**[4] - While vulnerability assessments may reveal particular weaknesses of a corporate network, the penetration test ascertains whether reasonable defense measures are employed to protect the corporate network. There are many perceptions and definitions of penetration testing, however an overall definition is *"…a live test of the effectiveness of security defenses through mimicking the actions of real-life attackers."*[5] The test can be performed by outside consultants, auditors, or internal staff. Typically, it is a combination of staff and consultants. Care should be taken in the selection of consultants to ensure their integrity, experience, expertise, and financial viability. The integrity of sensitive corporate data should be protected. Non-disclosure agreements should be executed with all outside parties involved in the test.

   Who should conduct penetration testing? **-** Any corporate that maintains critical data on its internal network and/or utilizes the Internet to deliver or receive business services.

   How often should penetration testing be conducted? **-** Immediately on major changes in the corporate network and introduction of new services and applications. In lieu of those events, penetration tests should be conducted every 12 to 18 months to ensure ongoing network integrity.

   The scope of the penetration test usually consists of external and internal penetration attempts. Attempts are made not only to compromise the corporate network through technical means, but also to use social engineering[6] techniques to obtain physical access, system passwords, and organizational information that will assist intruders in compromising the network.

   Penetration test results should be carefully evaluated. The failure to penetrate should not lead to a false sense of security. A successful attempt should be utilized constructively to improve network strength. A key measure of an effective security is employee reaction to the test. Were system administrators aware of unusual activity? Did monitoring software and systems provide prompt alerts? Did the office staff report attempts by outsiders to either gain physical access or confidential corporate information? These are key indicators that security has become more than a policy and is being integrated into the organization.

Conclusion - The key to effective risk management of technology is to identify the critical components and to develop a strategy to protect them. An effective strategy is one that identifies weaknesses, effects corrective action, integrates security into the entire organization, and establishes a pro-active surveillance program. OCCU recognizes that security programs, as well as their implementations will vary. These guidelines are intended to convey, in general, what is expected when information systems reviews are assessed during examination and other supervision contacts.

[4] A well-rounded article on penetration testing is "Penetration Testing Exposed" by George Krutz and Chris Prosise, at www.infosecuritymag.com/articles/sept00/.

[5] Quoted in "A Strategic View of Penetration Testing" by Eugene Schultz in Information Security Magazine, September 99 issue.

[6] Social engineering is non-technical hacking, exploiting human behavior to learn how to get people to give you information.