Information Security Checklist

Today's heightened awareness of the need to secure IT infrastructures and protect mission critical data is leading more and more organizations to reevaluate their security practices. To help you determine how your security program stacks up, infosecurity guru Ken Cutler has developed this security checklist:

1. POLICY: Has management provided the necessary leadership and reduced liability by issuing comprehensive information security policies, operating procedures, and associated responsibility statements?

2. EMPLOYEE ACKNOWLEDGEMENT: Are all employees and contractors required to provide written acknowledgement of their understanding and acceptance of the organization's information security policies?

3. CONFIDENTIALITY AGREEMENTS: Has the execution of properly signed confidentiality agreements been verified before proprietary and/or sensitive information is disclosed, in any form, to individuals outside the organization?

4. PHYSICAL SECURITY: Are buildings, paper records, and sensitive IT resources (e.g., computer and network equipment, storage media, wiring closets) within them properly secured from unauthorized access, tampering, damage, and/or theft by an intruder with malicious intent?

5. BUSINESS RESUMPTION PLAN: Does the organization have a documented and frequently tested business resumption plan for critical computer system and associated office support infrastructure that includes frequent system backups, off-site data backup storage, emergency notification, replacement IT and office resources, alternate facilities, and detailed recovery procedures?

6. ANTI-VIRUS: Are all computer systems protected with up-to-date anti-virus software and other defenses against malicious software attacks?

7. INTERNET SECURITY: Are all dedicated connections to the Internet and other external networks properly documented, authorized, and protected by firewalls, intrusion detection systems, virtual private networks (or other forms of encrypted communication,) and incident response capability?

8. REMOTE ACCESS: Are modem and wireless access point connections known, authorized, and properly secured?

9. PASSWORDS: Have all vendor-supplied, default passwords, or similar "published" access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products been changed or disabled?

10. SOFTWARE PATCHES: Are security-sensitive software patches, including the removal of unnecessary sample application software, promptly applied to systems that are accessible to users outside of the organization?

11. DATA PROTECTION: Is sensitive, valuable information properly protected from unauthorized access, including Windows network file shares and undocumented (desktop) Web and FTP servers?

12. AUDITS AND VULNERABILITY TESTING: Are all computers and network devices (e.g., routers, and switches) within your organization regularly tested for exploitable vulnerabilities and any unauthorized (or illegally copied!) software?

A negative or unsure response to one or more of the above questions places an organization in a position of unnecessary risk, not only to heightened possibility of direct financial loss and/or public embarrassment by a security incident, but also the loss of confidence and creditability in the organization.

Reprinted with permission from MIS Training Institute's TransMISsion Online. For a complete list of information security seminars and conferences available from MIS, go to: www.misli.com.