



Safeguarding Information for the Security Professional



As every security professional knows, an organization needs to effectively communicate in order to be successful. This may involve revealing company specific information, not only to employees and suppliers, but to potential customers in the interactive global marketplace. With this in mind, the following hints are provided for safeguarding your company resources, while at the same time maintaining your competitive edge.

Getting Down to Basics

- Obtain support for information security from senior management.
- Do not waste resources protecting that which does not require protection.
- Identify which information should be protected and for how long.
- If extremely sensitive, material should be hand-carried or transmitted using encryption techniques.
- To dispose of sensitive material, shred or make it unreadable.
- Valuable company information must not be left unattended in hotel rooms. This includes hardcopy and computer disks.
- E-mail and voicemail passwords must be protected and changed frequently.
- All sensitive materials must be removed from conference rooms and chalkboards and whiteboards erased after meetings.
- Where possible, conduct background investigations on all individuals with access to sensitive information.
- Obtain nondisclosure agreements from employees, vendors, and others with access to proprietary information.

Taking the Next Step

- Determine of monetary/competitive value of your information.
- Develop information safeguarding guidelines that are practical and user friendly.
- Get user input and buy-in when developing an information security program.
- Ask knowledgeable employees what should be protected; they know the market and the competition.
- Form a partnership with the organization's legal and information systems departments to better address information security issues.

- Identify and get the cooperation of senior stakeholders in key areas, such as technology, finance, personnel, and marketing.
- Train and periodically remind - from the first day of work through the exiting process - the appropriate people why certain information needs protection and of the guidelines used to protect it.
- Work with management to decide what access will be given consultants, subcontractors, and joint-venture partners.
- Partner with the legal department and other to develop a process to review employee publications, such as papers and speeches including those to be placed on the Internet.
- Ask new employees if they are obligated under any confidentiality or nondisclosure agreements.
- Use annual performance reviews to remind employees of their obligations.

Always Remember

- The disgruntled employee is the greatest threat to your organization.
- Telephone conversations, both fixed and mobile, are vulnerable to intercept.
- Information regarding the movement of your company aircraft, including routes and destinations, is available for sale on the Internet.
Be knowledgeable of your organization's physical assets, information assets, and vulnerabilities.

This information was prepared by the Safeguarding Proprietary Information Committee of the American Society for Industrial Security. For more information or to obtain a brochure, please call (703) 874-4122.