

<b>Types of Information Security</b>	
<b>Type of Security</b>	<b>Description</b>
<b>Physical Security</b>	<p>The first threat to an organization's information systems and data is unauthorized access to sensitive areas or information by persons, equipment, or materials. Areas of concern include anyplace where information is stored—on paper, on computers, or in other forms. The following are examples of physical security measures:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Limit the number of building access points.</li> <li><input type="checkbox"/> Use access identification systems such as employee badges, card readers, keypads, and biometric identification.</li> <li><input type="checkbox"/> Restrict access to information storage areas.</li> <li><input type="checkbox"/> Control delivery and removal of materials, equipment, or supplies.</li> <li><input type="checkbox"/> Train employees in security and vigilance.</li> </ul>
<b>Cybersecurity</b>	<p>A vulnerability in the cyber world is a "hole" through which a threat gains access to protected information that is stored electronically. Common cyber vulnerabilities include hackers, malicious code (viruses, spyware, worms, etc.), peer-to-peer software (file sharing, Internet meeting, or chat messaging programs), loss of removable media, and passive threats (natural hazards, power failures, software glitches, human error). Use measures such as the following for cyber protection:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Firewalls and virus protection systems.</li> <li><input type="checkbox"/> Information encryption software.</li> <li><input type="checkbox"/> Computer access control systems.</li> <li><input type="checkbox"/> Computer security staff background checks (at initial hire and periodically).</li> <li><input type="checkbox"/> Password procedures.</li> <li><input type="checkbox"/> Backup systems and disaster recovery plans.</li> </ul>
<b>Data Security</b>	<p>All employees play an integral role in data security—keeping their organization's information from ending up in the wrong hands. The following are suggested measures for handling data:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Store sensitive information where access control measures prevent unauthorized access.</li> <li><input type="checkbox"/> Never leave sensitive information on communal printers or email it to unauthorized individuals.</li> <li><input type="checkbox"/> Minimize and control print copies that could fall into the wrong hands.</li> <li><input type="checkbox"/> Avoid discussing cases or sensitive data on elevators where you might be overheard by other passengers.</li> </ul>