Security Controls

Instructor: Technology plays significant roles in everyday functions, and with it comes threats of intrusion, data theft, and other disruptions. Services, applications, and infrastructure have countermeasures applied to decrease the likelihood or impact of these threats. Security controls are a form of these countermeasures - they are safeguards that address security risks to information security assets.

Controls are classified and categorized according to how they are implemented. The classes are management, operational, and technical: Management focuses on managing risk and information system security; such as policies. Operational are primarily implemented by people; like a security guard verifying building access. Technical are the class of controls that are primarily implemented through components of a system - hardware or software. Examples include firewalls and intrusion detection systems.

The categorization of controls is according to function, or goal of the countermeasure:

Preventative controls are measures put in place to prevent a threat from occurring; such as locks to prevent unauthorized physical access, or antivirus software to prevent malware.

Detective controls detect and report an unauthorized or undesired event, or attempted event. Log monitoring, motion detectors, and file integrity checkers are examples of detective controls.

Deterrent controls discourage security violations. Security cameras installed in plain view, or a pop-up warning that a workstation is being monitored are deterrents; neither will stop an incident, but meant to deter.

Corrective controls respond to and fix an incident and limit or reduce further damage. Procedures for removing a virus from an infected system, or a security guard noticing an unlocked door and locking it are examples of corrective controls.

Recovery controls are for after an incident or event has occurred. Most disaster recovery activities fall within this category. Restoring data from backup tape after a disk failure would be a recovery control.

Compensating controls provide an additional or alternative to a typical control that is not suitable or sufficient. For instance, a server is unable to have antivirus software because it interferes with another application, so that server is isolated on its own network segment and has increased monitoring.

Implementing controls and prioritizing the security of data and systems is of national concern. The Federal Information Security

Management Act, FISMA, requires federal agencies to protect information and the systems that support operations. It specifically mandated the creation of federal standards for categorizing systems based upon risk levels, and establishing minimum security requirements for each category.

In response, NIST published those standards as: FIPS 199 Standards for Security Categorization of Federal Information and Information Systems and FIPS 200 Minimum Security Requirements for Federal Information and Information Systems.
FIPS 200 refers to NIST special publication 800-53 for the actual requirements.

NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organization, contains the security and privacy control requirements for federal organizations and information systems. The security control catalog is organized into families along with the minimum controls for a low, moderate, or high-impact information system. The minimum controls, or baseline are a starting point for selecting security controls; and then tailored according to agency-specific priorities.

No single control or countermeasure will protect from all threats. However, assessing risks will aid in appropriate control selection. Part of that is identifying threat vectors and attack surfaces within. The threat vector is the route an attacker uses to attempt a compromise. The attack surface are the vulnerabilities that may be exploited via that route.

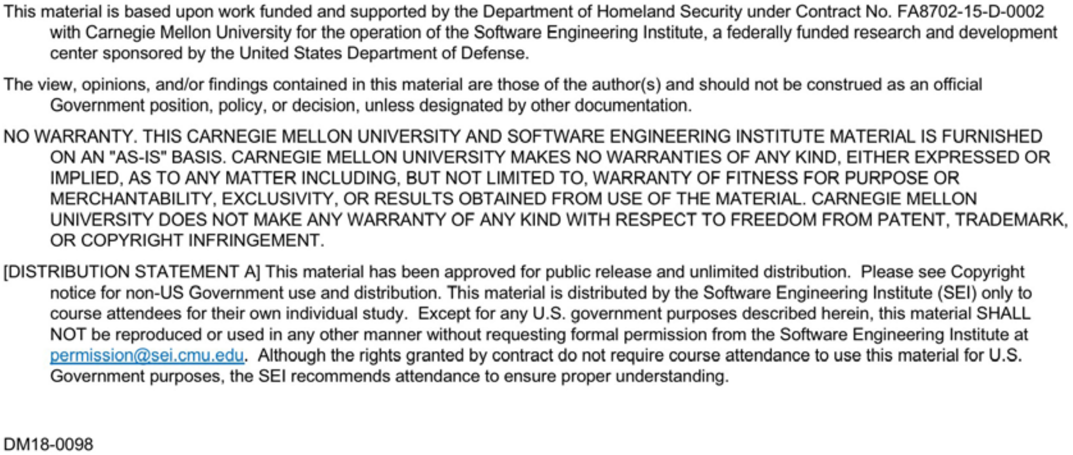
If email is a threat vector, then the attack surface could include vulnerabilities like naive users, unencrypted messages, and dated antivirus signatures.

Threats can use multiple threat vectors. Malware for instance can infect through an email attachment, a malicious link on a website, or through an infected removable device. Common threat vectors where intruders attempt to circumvent defenses include: Network, Web applications, Email, Business applications, Mobile devices, Remote access, Physical access, end users.

Applying countermeasures is a defense-in-depth, layered approach where if an attacker bypassed one control, it shouldn't provide keys to the kingdom. Security is pervasive, built into all systems at all levels.

Security controls are implemented to mitigate threats an entity may be vulnerable to. In order to apply appropriate countermeasures, risks and their impact are assessed. There are several resources for staying abreast of emerging threats and what industry, service, or application they apply to. As well as guidance for selecting and applying appropriate security controls. Protecting information assets is vital to the survivability of an organization.

Notices



This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM18-0098