THE NATIONAL CYBERSECURITY SOCIETY

How To Select Access Controls

DID YOU KNOW?

- Identify your critical business assets
- Include in the inventory both tangible and intangible assets - such as your IP
- Keep the list accurate, update each year
- Selecting a control(s) is the result of a risk assessment
- Backups are a recovery control
- Segmentation of duties is a preventive control
- If you have an incident - report it to us via our AIS portal to ensure protection against liability under the Cybersecurity Information Sharing Act of 2015.

Controlling access to your critical business assets is an important step in implementing your business' information security program. Access controls protect employees, customers, intellectual property as well as other critical assets your company relies on day to day.

The goal of a sound access control policy is to first identity your company's critical assets -- then establish access control rules to govern access. Many of these access control provisions are probably already in place at your business --- you lock the door, password protect business applications, back up data and define acceptable use policies.

The first step of a successful program is to document your risk and produce an accurate inventory of the assets you want to protect. This inventory should include both tangible and intangible assets. This inventory should be kept in a secure location as well as have a backup in the event this inventory is lost or stolen. The NCSS has developed an inventory tool to assist you in your efforts - see our Data Management Strategy. Aligning the inventory against the risks and likelihood of events occurring, will guide you in your access control decisions. In some cases you might have several controls protecting the asset (that is ok). An example of the approach is described below:

Asset - Threat - Likelihood - Risk = *Control(s)*

"Customer Database" - Theft by Hacker - Moderate to High - High Impact = *Limit employee access to file by password protection; encrypt data; store backup an alternative site.*

CONTROL 1: DIRECTIVE

Directive: Controls that define acceptable rules of behavior;

Examples: business policies; employee handbook; social media behavior; acceptable use policy; authorized personnel only signs; configuration standards

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

HOW TO SELECT ACESS CONTROLS continued...

CONTROL 2: DETERRENT

Deterrent: Controls designed to discourage people from violating your company directives;

Examples: policies, warning banner, surveillance notice, ADT sign;

CONTROL 3: PREVENTATIVE

Preventative: Controls implemented to prevent a security incident or data breach:

Examples: password login, two-factor authentication; fence; combination on a safe; access control list that designates only certain users have access;

CONTROL 4: COMPENSATING

Compensating - controls implemented to substitute for the loss of primary controls and mitigate the risk:

Examples: supervision over employee actions, job rotation, logs, CCTV, keystroke logging, layered defense, segmenting your network, HTTPS, SSL

CONTROL 5: DETECTIVE

Detective - controls designed to signal a warning when a security incident has occurred;

Examples: review violation reports; activity logs, guards, CCTV, data loss prevention reports.

CONTROL 6: CORRECTIVE

Corrective - controls implemented to remedy a situation or mitigate damage

Examples: terminate an employee, unplug, isolate or terminate connection, fire extinguisher

CONTROL 7: RECOVERY

Recovery - controls implemented to restore conditions to normal after a security incident.

Examples: Disaster recovery plan, backups, rebuild and restore

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.