Cyber Security Control Types

It is known what to defend (using information classification) and where to defend it (cyber defense points). But it is important to know how to defend it. There are 4 major categories of security controls that can be used when constructing cybersecurity protection:

- Physical
- Technical
- Procedural
- Legal (also referred to as regulatory or compliance controls)

Physical Security - measures designed to deter, prevent, detect or alert unauthorized real-world access to a site or material item.

If some gold bars need to be kept safe, they can be placed in a locked, alarmed and isolated vault that would make it extremely difficult to steal. If there is a digital memory card, packed with sensitive information but not attached to anything else, exactly the same possibilities remain.

At this point, although the data is electronic, it is in a physical form.

Potentially, this memory card is more secure than a printed document, because although it could be stolen, it needs to be inserted into a device before it can be read.

Without physical security, other, more sophisticated types of cyber defense become less relevant. If someone can physically get to the memory card, he or she can still steal or destroy the physical item.

The same thing can happen with any critical part of a digital landscape. If someone can gain physical access to part of the digital landscape, he or she can cause disruption, steal it, or use it to gain access to even more areas.

Procedural control – an instruction during a sequence of required steps to limit how something is or is not permitted to be used.

An example of a procedural control is to require a minimum of 2 authorized people to approve any access request. Procedural controls use any process (enforced or otherwise) whose purpose is to help strengthen a security position.

Technical control – the use of an electronic or digital method to influence or command how something like a digital device can or cannot be used. For example, removing the ability to cut or paste information on a smartphone is an example of a technical control.

Almost all technical controls are ineffective if physical access can be gained to restricted equipment.

If returned to the memory card example, if the information on the card is encoded, that would be an example of a technical security control. Such would have been done electronically to secure the item. It might not prevent the theft of the item but it could prevent the information from being exposed.

Legal control – the use of legislation to help promote and invest in positive security methods and also to deter, punish and correct infringements.

Whenever it is heard that a large financial penalty being imposed on an organization, this is an example of the consequences of not meeting a legal control requirement. Many companies seek to pass some of their legal financial responsibilities onto their employees or suppliers as an incentive to promote good practices. It is also normal for any breach in legal controls to result in disciplinary action.