Protect

Cybersecurity Control Types

We know what to defend (using information classification) and where to defend it (cyber defense points). We still need to know how to defend it.

There are 4 major categories of security controls that can be used when constructing cybersecurity protection:

1. Physical
2. Technical
3. Procedural
4. Legal (also referred to as regulatory or compliance controls)

If I want to keep some gold bullion safe, I can place it in a locked, alarmed and isolated vault that would make it extremely difficult to steal.

If I have a digital memory card, packed with sensitive information but not attached to anything else, I have exactly the same possibilities.

At this point, although my 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 my memory card, he or she can still steal or destroy the physical item.

> ***physical security*** *– measures designed to deter, prevent, detect or alert unauthorized real-world access to a site or material item.*

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

I recall auditing a research site. The main facility where over 100 people worked was in a physically secure office space. The entire building's network, on the other hand, was managed in an unlocked cupboard, propped open by a cardboard box (to keep the cupboard cool) in the main, open and unmanned lobby.

Anybody could have walked in off the street, unchallenged, and could have pulled out 2 wires and stopped all 100 people from working. This individual could also have plugged something into the network and would thus have easily defeated all the technical defenses that were in place at that location.

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

If we return to our memory card example, if I encoded (encrypted) the information on the card, that would be an example of a technical security control. I would have done something electronically to secure the item. It might not prevent the theft of the item but it could prevent the information from being exposed.

> ***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 that can be used to minimize security risks.*

The next control type to consider is procedural.

> ***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.

The last category can be referred to as legal, regulatory or compliance controls.

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

Whenever you hear about 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.

We have only covered these 4 areas very briefly. But it is important to understand that any effective cybersecurity approach must be effective in all four control areas.

Maintaining technical controls alone will not result in effective cybersecurity.

Each time a new type of information is identified, the assets and mechanisms it will travel through also have to be identified. Any additional security protection requirements for those assets can then be consistently identified and implemented.

However, technologies and services are often deployed without the right controls and protection. To cope with this issue, we cannot rely on protection alone. Our cyber framework must also be able to actively detect and respond to these situations.