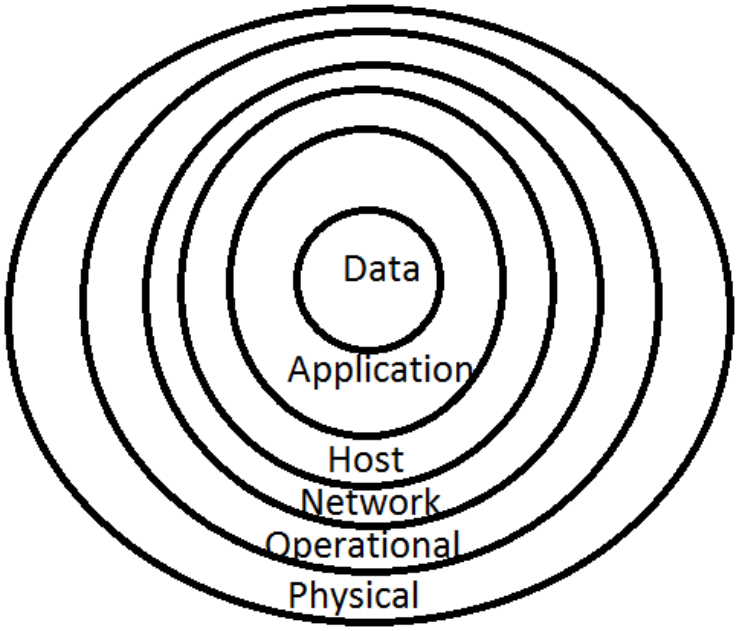
Lesson 3: Defense in Depth and related concepts

by Justin David Pineda

Defense in Depth



We have agreed that we protect data/information in Infosec. And as we have discussed in Lesson 1, the scope of Infosec is very broad and IT Security is just part of it. We have also learned in Lesson 2 that preventive controls are incomplete without detective controls and response. With former concepts discussed, a more concrete and concise security architecture is formed- Defense in Depth.

The concept of Defense in Depth states that in order for anybody to access the data, it should pass layers of security first. Security controls may vary but it should be in layers.

For example, if you want to access the bank database, you need to pass through frisking of security guards, inspection of bags and proper identification when entering the bank premises. That is what we call Physical Security.

When you enter the premises, you are required to wear your ID at all times. If you are a visitor, a security personnel is required to accompany you wherever you go within the premises. That is the next layer called the Operational Security.

If you connect to their wireless network and your laptop cannot access the Internet because of MAC filtering, that is an example of Network Security.

When desktop computers have disabled USB ports to prevent spread/download of virus, that is an example of Host Security.

When you need to enter a username and password to gain access to your account, that is an example of Application Security.

Diversity of Defense

The Diversity of Defense security concept is quite tricky. Management will always want a cost-effective IT infrastructure setup. For example, Huawei, a known networking product, might offer an IT infrastructure package that may be very appealing. Let's say they offer the whole IT infrastructure with X pesos. The management may be lured to buy the package because of the cost. However, as an information security professional, you should weigh the possible security issues that may take in place.

In Diversity of Defense, you are compelled to buy different brands of network and IT devices such as firewall, switch, router, etc. But assuming you plan to buy different types of devices, the cost may double (2X pesos) compared to the X pesos if you have a single brand.

So what is the advantage of this concept?

If a vulnerability in Huawei firewall is found, no matter how many Huawei firewalls you have, then your network is vulnerable to that particular attack. You can simply say that the cost of information disclosure is way more expensive than the implementation of diversity of defense when a single proprietary vulnerability is exploited.

Security through Obscurity

If we say that a company is implementing security through obscurity, can we consider it secured? In Security through Obscurity, we rely on the idea that nobody will think that some valuable asset is hidden in an obscure place.

For example, will anybody think that there's 1M pesos stored underneath the driver's seat of my car? What are the odds, right? But if I accidentally left my car unlock and somebody randomly opens the door of my car, is my asset still secured?

Security through obscurity is simply hiding something. But hiding something without proper safeguards has no security at all.

Cost-Benefit Analysis (CBA)

In information security terms, CBA refers to the weighing of the cost of safeguards to the value of asset. As a rule of thumb, you are not supposed to buy a safeguard that is more expensive than the asset.

For example, you won't buy a vault that is valued at 20,000 pesos to safeguard a Timex watch from a buy 1 take 1 sale worth 2,000 pesos. The thief will probably steal the safeguard instead of the asset in it.

----- NOTHING FOLLOWS -----