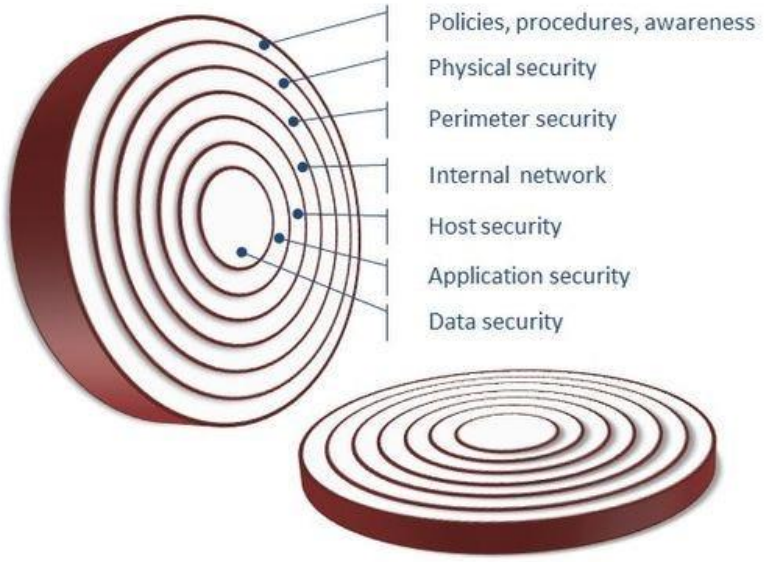
Shawn Edie – Director of Information Technology

Security like an Onion

Network Security can be an overwhelming experience. If you think of it like the layers of an onion, you can visualize what you need to do.



So let's discuss each of the layers.

- Policies, procedures, awareness – This layer is Security Awareness Training for your users, Computer Use Policy, Disaster Recovery Plans, Business Continuity Plans
- Physical Security – Are all your Network cabinets in locked key-controlled rooms or cabinets? Do you regularly check access logs for the rooms?
- Perimeter Security - This is normally your Firewall. It is highly recommended that you use a Next-Gen Firewall. These firewalls do additional scanning of the information that travels through it whereas a standard firewall does not.
- Internal Network - This is your physical network. Do you have all unused ports disabled on your switches? This can be done by physically patching and un-patching connects or using 802.1x
- Host Security – This is your system firewall, Anti-Virus, Malware, and Patch Updates. This layer is very important. If you don't keep your systems up to date and have a Next-Generation Anti-Virus then you will get hit with infections. This includes all servers. You have to keep all your systems up to date and Security tools installed on them.
- Application Security – This is your domain login and application Login. One of the most important items at this layer is multi-factor authentication(MFA). You need to be sure that when a user is removed their access is shut off immediately. You need to have a Password Policy where you are forcing all users to change their password every 30 to 90 days. They are forced to use password complexity. You also need to only give rights to users for what they need not what they want.
- Data Security – This is your backup and Shadow Copies. Make sure that you have accurate and up-to-date backups of all your data. Test and verify that these backups are good. If you don't test ahead of time then when you need it you won't have it!

So as you can see as you allow an attack to get into each of your layers, the further in the more damage that it will cause. I have created a checklist to make sure you are ready for the next attack.

Security Checklist

If you answer no to any of these questions you may be vulnerable to an attack.

- Do you have Security Awareness Training?
- Is your firewall a Next-Generation Firewall?
- Is your firewall software up to date?
- Do you have all your Network equipment physically secured so that no one can access it without a key?
- Do you have physical network ports active on your corporate network?
- Do you have a SPAM filter and is it actively monitored?
- Do you have a WEB filter and is it actively being monitored?
- Do you have all of your workstations, laptops and Servers current on all updates?
- Do you have all of your applications current on all updates?
- When an employee leaves the company are there external logins disabled within 24 hours or less?
- Do you have Anti-Virus installed on all machines including servers?
- Do you have a Next-Gen Anti-Virus that does not just rely on virus definition updates?
- Do you have a password policy that requires passwords to be changed every 30 to 90 days and has complexity requirements?
- Do you have a password policy that does not allow users to use the same password for x amount of uses?
- Are ALL your users required to change their password according to your password policy?
- Have all shared logins been removed from your systems?
- Are you regularly doing external vulnerability scans on your systems?
- Are you regularly testing your backups?
- Do you have MFA fully deployed?
- Do you have a Security Operations Center (SOC) solution?
- Do you have a Disaster Recovery Plan(DRP)/Business Continuity Plan(BCP)?
- Have you done a Table-Top exercise for the DRP/BCP plan?
- Do you have adequate cyber insurance?