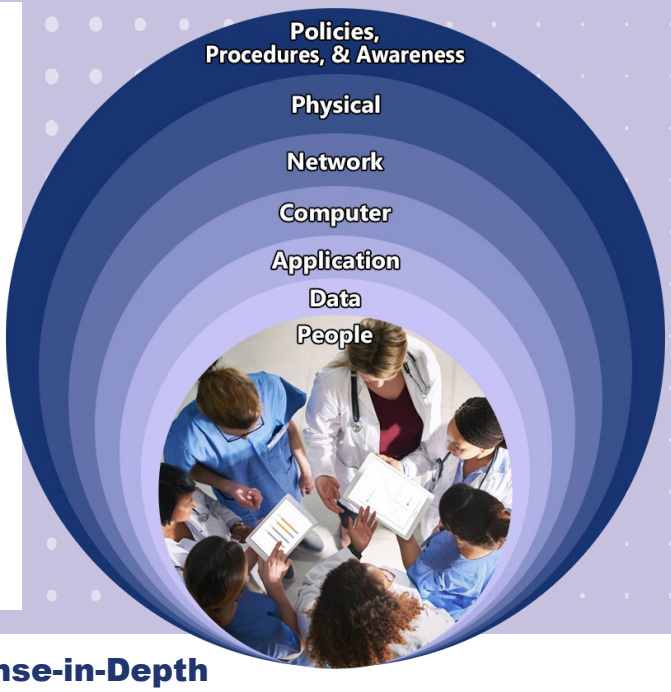
Defense-in-Depth

Office of Information Technology
Division of Information Security
APRIL 2022

What is Defense-in-Depth?

Defense-in-depth is an implementation of cybersecurity in layers so that if one protection fails, others are available to maintain a secure posture. Using different kinds of security is an important aspect of defense-in-depth because defeating dissimilar kinds of security requires attackers to use different tactics. This takes more time and such effort may be enough to thwart a malicious actor. The attacker will then try to find another target not implementing defense-in-depth or implementing it poorly. The graphic on the right gives one representation of how different protections secure IHS assets. Please notice that people are at the very core of protection mechanisms; personnel is the last line of defense in any security solution.



Benefits of Defense-in-Depth

Overall, defense-in-depth supports the IHS mission by protecting our employees, facilities, infrastructure, and data. Each component of our layered cybersecurity defense benefits specific components of the Agency's IT systems. For example, employees are required to take cybersecurity and privacy trainings when they first start at IHS and annually thereafter. Training is one way we develop user awareness, as shown in the outer ring of the defense-in-depth graphic. Requiring all system users to take the same trainings provides everyone with the same knowledge in the short term, but also fosters, over time, a culture where cybersecurity- and privacy-focused behaviors become part of what users expect of themselves and others.

Going a few layers into the graphic above for another example, network defenses limit access to the IHS intranet and its resources in accordance with approved policies and procedures. These defenses include ensuring only approved devices can connect to the network and IHS uses mechanisms to identify users and grant their authorizations. Even in the case of user-access compromise, no single IHS user has access to all IHS applications or data. Defense-in-depth designs protect system assets should previous defense layers fail or otherwise fall short.

Implementing defense-in-depth at the network layer can keep trusted users from mistakenly accessing system resources without authorization. For instance, only specific personnel are permitted to view patient medical records. Using role assignments, access managers can ensure that no one can see information beyond what is required for the scope of their job supporting the IHS mission.

Implementing Defense-in-Depth

Defense-in-depth is such a part of our workdays that we usually do not think about it unless there is a problem or we see suspicious activity. From using PIV cards to access facilities and laptops to limiting permissions to read-only data, IHS implements layers of security to protect our employees

and support the IHS mission. While implementation requires some technical expertise, successful execution requires the support, attention, and commitment of every single employee. Every user needs to practice good cyber hygiene all the time. This means keeping up with security trainings and maintaining control of every IHS asset for which you are responsible.

Layer by layer, here are some ways you can apply cybersecurity defense-in-depth in your personal life and on your personal devices.

Awareness

Stay up to date on cybersecurity incidents and take note of the ones that may affect you or your loved ones. This can include notifications about merchant breaches or device security issues.

Physical

Keep your home and vehicles secure. Lock your doors and secure other entry points. Consider investing in systems that will notify you and/or authorities of suspicious activity around your home.

Network

Maintain strong passwords for your home network and use an abundance of caution when connecting to unknown or public networks. Use your mobile service provider's hot spot instead of an untrusted wireless network.

Computer

At all times, control your personal devices, like laptops and mobile phones, or keep them in a secure location to avoid avoid theft or loss of information. Make sure they are password or PIN protected to keep unauthorized persons from gaining access.

Application

Make sure to keep your important applications, such as finance or health, secure from prying or curious eyes. Whenever possible, use a combination of complex passwords with multi-factor authentication to access applications that contain sensitive information, and make sure other authorized account users are doing the same.

Data

Store your most important data offline or in secure online storage. If your data is ever lost or compromised, having a trusted, up-to-date backup will make it easier to restore your systems and information.

People

Practice good cybersecurity consistently and encourage your family and friends to do the same. Good cybersecurity practices help to keep us, and our information, safe.

Conclusion

Whatever mechanisms IHS uses to enforce defense-in-depth, they aim to protect the Agency's greatest asset, our people. IHS relies on you, our people, to be the last line of defense in case all other protections perform inefficiently or not at all. Please do your part to adhere to policies, remember your training, and help maintain a culture of security and privacy to protect our mission and the communities we serve.

If you have any questions about this article, please contact Cybersecurity@ihs.gov. If you suspect an IT incident has occurred, contact the Cybersecurity Incident Response Team at Incident@ihs.gov.

Please remember, the Information Systems Security Awareness (ISSA) training deadline of **June 3, 2022** is approaching. We encourage all IHS system users to complete their trainings at www.IHS.gov/ISSA as soon as possible.