An attacker can find many entry points into a given system or network and often explores several avenues of attack before finding success. Potential targets of an attacker include network protocols, network services, operating systems, Internet applications, network devices, and hardware environments. As a result, there are many potential targets to monitor regularly.

There is no single consistent way to enter a network environment because a network includes different elements and configurations. End users are always a favored target because they represent the greatest potential lapse in security measures. Internet-facing servers are another ideal target into the network, especially where virtual private network (VPN) laptop clients are involved. A malicious insider could also attempt to elevate privilege or unleash exploits from a portable universal serial bus (USB) drive.

From a defender perspective, you can never know where to expect an attack because an attack can originate anywhere and everywhere, including inside the network.

Consider what happens if countermeasures are missing or fail in the seven domains of a typical IT infrastructure:

1. **User Domain:** Weak password selections create an opportunity for attackers to obtain real accounts.
2. **Workstation Domain:** Company laptops are not encrypted and contain sensitive data that can be stolen.
3. **LAN Domain:** End users aren’t always savvy enough to determine genuine e-mail offers from convincing spam e-mails.
4. **LAN-to-WAN Domain:** File transfer protocol (FTP) servers are left open to store unauthorized third-party applications and data.
5. **WAN Domain:** Wide area network (WAN) gateways remain open to unauthorized connections made into or out of the network environment.
6. **Remote Access Domain:** Weak endpoint security on VPN clients exposes sensitive internal network resources to an unauthorized third party.
7. **System/Application Domain:** Unpatched server operating systems provide an opportunity for attack.

