

The Top 10 Things a CEO Should Know about Security: Protection Against Today's Hackers

1. **Stealing Passwords.** Passwords have been a security issue for a long time. Real protection with passwords can only be obtained by requiring employees to remember very long and complex passwords. Password theft, password cracking, and even password guessing are still serious threats to IT environments. The best protection against these threats is to deploy multifactor authentication systems and to train personnel regarding safe password habits.
2. **Trojan Horses.** A Trojan horse is a continuing threat to all forms of IT communication. Basically, a Trojan horse is a malicious payload surreptitiously delivered inside a benign host. The malicious payload can be anything. This includes programs that destroy hard drives, corrupt files, record keystrokes, monitor network traffic, duplicate e-mails, and more. Payloads can be grabbed off the Internet. In any case, your protections are automated malicious code detection tools, such as modern anti-virus protections and other specific forms of malware scanners and user education.
3. **Exploiting Defaults.** Nothing makes attacking a target network easier than when the target is using the defaults set by the vendor or manufacturer. Many of the tools and exploit scripts assume the target is configured using the default settings. Thus, one of the most effective and often overlooked security precautions is to simply change the defaults.
4. **Man-in-the-Middle Attacks.** All of us has been a target of man-in-the-middle attacks. This attack occurs when an attacker is able to fool a user into establishing a communication link with a server or service through a rogue entity. This entity is a system controlled by the hacker and has been set up to intercept the communication between the user and server without letting the user become aware that the misdirection has taken place. To protect against these attacks, avoid clicking on links found in e-mails and deploy Intrusion Detection Systems to monitor network traffic.
5. **Wireless Attacks.** Wireless networks have the appeal of freedom from wires. Wireless networks are inexpensive to deploy and easy to install. Unfortunately, the true cost of wireless networking is not apparent until security is considered. It is often the case that the time, effort, and expense required to secure wireless networks is significantly more than deploying a traditional wired network. Even if your organization does not deploy a wireless network, you may have wireless network vulnerabilities. To combat unapproved wireless access points, a regular site survey needs to be performed. These surveys are usually part of a security assessment.

6. **Doing their Homework.** Hackers, especially external hackers, learn how to overcome your security barriers by researching your organization. This process can be called reconnaissance, discovery, or foot printing. Once information is out on the Internet, it is always out there. This information could erode your security. The only way to manage uncontrollable information is to alter your environment so that it is no longer correct or relevant. Think of it as a new way to deviate from defaults or at least deviate from the previous known.
7. **Monitoring Vulnerability Research.** Hackers have access to the same vulnerability research that you do. They are able to read Web sites, discussion lists, blogs, and other public information services about known problems, issues, and vulnerabilities with hardware and software. The more the hacker can discover about possible attack points, the more likely it is that he or she can discover a weakness your administrator or service provider has yet to patch, protect, or even become aware of. To combat vulnerability research on the part of the hacker, you have to be just as vigilant as the hacker. Your administrators or service providers should be looking for the problems in order to protect against them just as intently as the hacker is looking for problems to exploit. This means keeping watch on discussion groups and Web sites from each and every vendor whose products your organization utilizes. Plus, you need to watch the third-party security oversight discussion groups and Web sites to learn about issues that vendors are failing to make public or that don't yet have easy solutions. These include places like securityfocus.com, US CERT, hackerstorm.com, and hackerwatch.org.
8. **Being Patient and Persistent.** Hacking into a company network is not typically an activity someone undertakes and completes in a short period of time. Hackers often research their targets for weeks or months before starting their first interactions. Keep in mind that the goal is to gain entry subtly so that your IT department is unaware that a breach has actually taken place. Hacking is most successful when performed one small step at a time and with significant periods of time between each step attempt. Likewise, protecting against a hacker is also about patience and persistence. You must be able to watch even the most minor activities on your network with auditing processes as well as an automated IDS/IPS system. Follow best business practices recommended by security professionals and keep current on patches, updates, and system improvements. Remember that security is not a goal that can be fully obtained; there is no perfect security environment!
9. **Confidence Games.** The good news about hacking today is that many security mechanisms are very good against most hacking attempts. Firewalls, IDSeS, IPSeS, and anti-malware scanners have made intrusions and hacking a difficult task. However, the bad news is that many hackers have expanded their idea of what hacking means to include social engineering. People are always the biggest problem with security because they are the only element within the secured environment that has the ability to choose to violate the rules. The age-old problem of people exploiting other people by taking advantage of human nature has returned as a means to bypass modern security technology. Protection against social engineering primarily involves education. Training personnel about what to look for and to report all abnormal or awkward interactions can be effective countermeasures. But, this is only true if everyone in the organization realizes that they are a social engineering target. In fact, the more a person believes that their position in the company is so minor that they would not be a worthwhile target, the more they are actually the preferred targets of the hacker.

10. **Already Being on the Inside.** All too often when security and hacking is discussed, it is assumed that the attack comes from outside of the network by some unknown individual. However, studies have shown that a majority of security violations actually are caused by internal employees. So, one of the most effective ways for a hacker to breach security is to be an employee. This can be accomplished in two ways. First, the hacker can get a job at the target company and then exploit access to the network once they gain the trust of the organization. Second, an existing employee can become disgruntled and choose to cause harm to the company as a form of revenge or retribution. In either case, when someone on the inside decides to attack the company network, many of the security defenses erected against outside hacking and intrusion are often ineffective. Instead, internal defenses specific to managing internal threats need to be deployed. This could include keystroke monitoring, tighter enforcement of the principle of least privilege, preventing users from installing software, not allowing any external removable media source, disabling all USB ports, extensive auditing, host-based IDS/IPS, and Internet filtering and monitoring.