

# APPROACHES FOR SECURING MODERN COMPUTER NETWORKS AGAINST CYBER ATTACK

Jaylyn Jensen,  
Director Government Relations,  
Washington, DC, 202-624-3538  
jaylynj@us.lenovo.com

Stacy Cannady, CISSP  
Product Manager, Security Solutions for Lenovo  
Morrisville, NC, 919-294-5944  
[scannady@us.lenovo.com](mailto:scannady@us.lenovo.com)

## SUMMARY

Cyber crime costs corporations, small businesses, government agencies and consumers billions of dollars each year. A person who has never logged onto an Internet website is still at risk if the entities who have their data (doctors, banks, retail stores, etc.) use computer networks. Modern computer networks feature several enabling weaknesses that make the task of a cyber attacker much easier. This fact sheet discusses two specific cyber security weaknesses, and ways to improve their security posture.

## COMPUTER AND USER IDENTIFICATION

Computers are not required to have unique identities that can be evaluated at the time a computer attempts to connect to a target network. The Department of Defense does not allow just anyone to walk into an installation because the person shows up at the gate. The person must identify himself and must be found to be authorized to be present at the installation. *Computer networks do not make a similar demand of a computer that demands access to a network.*

Off-the-shelf technology exists today that can provide a unique identity to a computer and which can then be evaluated by a network when a computer tries to connect. TPM, or Trusted Platform Modules, use a kind of digital passport or “certificate” that can be installed in authorized PCs of that network, thereby allowing only authorized PC’s access. Further, these digital certificates can be issued to specific *users* of authorized PCs, and used in much the same way. When the digital certificate is demanded, the TPM requires the person at the keyboard to authenticate before allowing access. If a user of an authorized PC, cannot show they are an authorized user of that PC and that network, the connection can be denied. This approach blocks one significant vector of cyber-attack - the hacker trying to break into the private network of a victim company or agency.

## TARGETED COMPUTER THEFT

Another method of attack is to target and steal laptops of interest. The news is full of stories about missing or stolen laptops containing customer or personal data. Some data suggests 5% of company laptops go missing each year. A targeted theft might not even be identified as such, just one more randomly stolen PC. In a case like this, the data on the drive is the target.

The foundation of defense for this data is encryption. Computer encryption with either hardware or software, can be used to create a kind of cyber safety deposit box. The information that is encrypted can only be accessed by someone holding the correct electronic key.

- Example. If someone steals a computer with an encrypted drive, while the PC is turned off or in hibernate, then the data on the computer cannot be accessed and is SAFE.

Within the security industry there are well understood practices for the use of encryption. New encrypting drives add an additional cost of approximately \$25 to the purchase of a computer, and can provide encryption that the NSA sanctions as good enough for Top Secret clearance. However, encryption can also cause problems.

- Example: If the electronic key is lost, or the drive is damaged or the password forgotten, the data on the drive is gone, FOREVER.

Encryption technology creates new security opportunities to provide inexpensive, yet very high quality protection for data on any laptop, when it is used correctly.

## LEVELS OF SECURITY

There are a broad range of opportunities that agencies and businesses can take to improve their security posture. Simple enforcement of security best practices, such as those required under the payment card industry (PCI) data security standard has value when considering cyber attack. The PCI Data Security Standard directs a company to implement a set of 12 security Best Practices in 6 categories and is considered good basic IT security. Similar to the value of an effective civil defense, these best practices create difficulties for an attacker.

Implementing cyber security procedures can be daunting, expensive and time consuming. Businesses who spend less on cyber security are easier to compromise and are therefore more attractive targets for attackers. In general, a company’s security policy is not a considered for access to big, important networks, (healthcare, banking, etc.). A company with weak security can be used by an attacker to gain access to those networks. Inexpensive and meaningful solutions for business especially small business, is an important part of securing intersecting computer networks.