



Information Security Standards for Success: 10 Steps to Protect Your Network

By Gerhard Lindenmayer, Chief Information Officer, DialAmerica

Today, information is a crucial asset for virtually every business. For competitive, operational and compliance reasons, extraordinary steps must be taken to securely protect it from being compromised – either accidentally or maliciously.

Following are ten key steps that companies can take to ensure the security of the data within their networks.

1. Effective security requires a “layered approach”

No single piece of hardware or software, and no set policy – regardless of how strongly it is worded – can ensure that your data will be safe. Don’t make the mistake of thinking that by installing a single new piece of equipment or software program that you will be fully protected. You won’t! You need to employ a comprehensive combination of technology, training, policy and enforcement for it all to work.

2. Encrypt....Encrypt...Encrypt!

No security solution is 100 percent foolproof. The most secured data center in the world without encrypted data is an accident waiting to happen. However, if one should experience a breach, but all the data is encrypted, it becomes much less of an issue.

There are different types of software that companies use for encryption. An effective and well-known standard tool is PGP, which stands for ‘Pretty Good Privacy’. There are also operating system-based encryption tools, such as Windows EFS – Encrypted File System. The more encryption services used, the tighter the security of data.

3. Implement security policies and enforce them

Security must become a company-wide mindset. Train your employees and hold them accountable for the data in their control. Use posters and visual reminders to let employees know that security is everyone’s concern.

4. Apply strong password protection

Implement and enforce a strong password policy by requiring that passwords consist of upper and lower case letters, numbers and special characters. Use token or “two factor” authentication wherever possible, especially in providing remote access to your network. A token can be a card, which generates a random unique number that changes every 60 seconds. Two-factor means that two separate pieces of information are required to get into the network. In some circumstances for access, three requirements are preferable, for example establishing a VPN (virtual private network) connecting through software and then using a unique password and a token. The more steps you take, the more secure your network will be.

5. Utilize and update a strong anti-virus solution

Use a well-known antivirus software and install updated virus definition files on a regular basis. This is accomplished by utilizing a “parent server,” that monitors and automatically

downloads the definitions when they are available. The new definitions can then be pushed out to your systems, ensuring you the most current protection on your network.

6. Prevent data from being removed by employees

To ensure that data cannot be removed by employees from your premises, strictly eliminate – or limit – their ability to use portable USB storage devices such as micro drives, memory sticks and CD/DVD drives. Also restrict the size of email transmissions wherever possible. Monitor all emails and set limits on sizes of emails to 1 MB. or smaller. If a staff member tries to send a larger file, the email should automatically be blocked.

7. Restrict Internet access

Limit the ability of employees to surf the Internet by filtering and allowing them to only visit sites that meet a true business need. Outside email sites add a potential threat to your network and leave your system more vulnerable, as they are notorious for harboring viral downloads. Therefore, it is advisable to block access to these services.

8. Install Operating System patches on a regular schedule

Engage the services of outside consultants to test, analyze and recommend proper security upgrades. Continuously harden your systems by removing or shutting down any nonessential programs or services from your systems, thus blocking any “back doors” to hackers seeking to gain entry to your private network.

9. Build and maintain firewalls and install intrusion prevention/detection systems and monitor their logs

Firewalls provide LAN segmentation, a Demilitarization zone (DMZ), and limit what services are accessible. Placing servers on a DMZ LAN segment behind a firewall, as opposed to a publicly-facing segment, is crucial as many of the filtering mechanisms in a firewall can limit access to specific services based on TCP/IP ports, IP addresses and/or protocols.

Intrusion detection alerts you to problems on the network while intrusion prevention shuts them out. An intrusion prevention/detection system strategically placed will greatly assist in protecting the network infrastructure and all hosts connected to it.

10. Conduct regular penetration tests with an outside service

At a minimum, have an annual penetration test conducted on your network by an outside source. This step will alert you to potential vulnerabilities. DialAmerica changes the vendor that conducts this test every year in order to make sure the procedures are completely accurate and unbiased. We allow companies to spend several days trying to get past our firewalls, infiltrate our network and extract data. They have never succeeded!

If your company uses credit cards for customer transactions, your servers and ports should be scanned on a quarterly basis in order to comply with the Payment Card Industry Data Security Standard (PCI). DialAmerica chooses to be more stringent and has the tests run monthly so that it can react more quickly to potential vulnerabilities.

###

DialAmerica, one of the nation’s largest teleservices company now in its 50th year, knows customer data. As a company that handles an average of 150 million calls a year for its clients, keeping customer information safe and secure is of prime importance. Maintaining the highest standards in data security is a badge of honor the company wears proudly.

Lindenmayer is a 24-year veteran of DialAmerica. Previously Lindenmayer was a Senior Analyst in the Technical Services division at Volkswagen of America where he began his career in Information Technology. He has a B.S. in Business Management from Saint Peter's College.