State of West Virginia
Cyber Security Tip

Septembr Newsletter

West Virginia Office of Information Security and Controls – Jim Richards, WV Chief Information Security Officer

Using Encryption for Data Protection

According to the Privacy Rights Clearinghouse, more than 19 million records have been involved in a data breach so far this year. Protection of data requires multiple layers of defense, and the use of encryption to secure sensitive data is a critical tool in this multi-layered approach.

Encryption scrambles a message or file so only the sender and the authorized individual with the decryption key can decode it. Encryption solutions generally encompass two types: hardware and software. Examples of hardware encryption include a pre-encrypted USB device or hard drive; software encryption consists of a program installed on a machine that encrypts some or all of the data on the system.

The list includes guidance for how, when and where encryption should be implemented in order to enhance security and data protection. Depending on your agency or organization, some of these methods of protection may already be in use:

- **Laptop protection** - Theft of laptops can result in unsecured information being used by a third party to gain access to bank accounts, mobile phones, internal networks, and other sensitive information. A stolen laptop can become a security risk if it contains confidential information or passwords. Enabling laptop encryption is a recommended way to reduce these risks, while ensuring that information cannot be easily retrieved. Laptops can be encrypted in various ways: encrypting specific directories and files or encrypting the entire hard drive (full disk encryption). Some analysts recommend using both forms of encryption on the same laptop as that is more secure than either method on its own. In the Windows 7 version of the Microsoft Operating System, the operating system contains BitLocker, also known as Whole Drive encryption, as one of its features. Minimally, file level encryption should be implemented; full disk encryption is a best practice.

- **Wireless networks** – The first line of defense for a Wi-Fi network is encryption, which encodes the data transmitted between your electronic device and the wireless access point. Unfortunately, most wireless access points ship with encryption turned off, and many owners of the wireless access points don't turn it on, leaving users completely exposed. If you haven't already, enable your home wireless access point's encryption, and use the strongest form supported by your network. The Wireless Protected Access (WPA) protocol and more recent WPA2 have supplanted the older and less-secure Wireless Encryption Protocol (WEP). It is highly recommended that your network support WPA2. Both WPA and WEP are considered to be significantly weaker, as the algorithms for those have been cracked.

- **Email** – It is important to realize that email and IM messages pass through numerous servers and routers before reaching their final destination. Standard email messages are sent in plain text, so it's possible for someone else to snoop and read them. When you encrypt mail, on the other hand, it makes the messages completely unreadable to anyone who doesn't possess a decryption key. There are several ways to encrypt email. Confidential or sensitive data should not be sent via email in clear text.

- **Removable Media** – CDs, DVDs, and USB flash drives are great for transporting files and documents back and forth from the office and to home or to a meeting or on a business trip. The portability though has disadvantages. These media are small and easy to lose or misplace. Your best defense is to encrypt the files on your removable media or use, where available, pre-encrypted removable media such as a pre-encrypted USB drive.

- **Smartphones, PDAs and other similar devices** – Gone are the days when a cell phone is used primarily for placing phone calls. Modern smartphones, PDAs, etc., can surf the Internet, email, text and take pictures and

videos. They have large amounts of internal memory capable of storing large volumes of information. Though this is undoubtedly convenient, it makes losing your phone a frightening prospect. With so much personal data at risk, and identity theft such a major concern, you must take steps to protect yourself. It is recommended that you enable the encryption features on your smartphone.

- **Media Card Encryption on Blackberries:**
  http://docs.blackberry.com/en/smartphone_users/deliverables/1487/Encrypt_files_on_a_media_card_422_187842_11.jsp

- **Data Protection in iOS Devices:**
  http://support.apple.com/kb/HT4175

- **Encryption on Android Devices:**
  http://support.google.com/android/bin/answer.py?hl=en&answer=1663755

A variety of encryption tools are available in the marketplace—some of which are open source--however, please note any solution you implement should be compliant with accepted industry standards. Given the current technology environment, you should minimally employ a 128-bit Advanced Encryption Standard (AES) solution.

For More Information

- MaximumPC: How To Erase Your Digital Footprint:
  http://www.maximumpc.com/article/features/how_erase_your_digital_footprint

- Washington Post: Beware of Privacy Policies: Time to Clean Up Your Digital Footprint:
  http://www.washingtonpost.com/lifestyle/style/beware-of-privacy-policies-time-to-hide-your-digital-footprint/2012/01/31/gIQADI7PnQ_story.html

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. ***Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.***

Brought to you by:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY

DIVISION OF THE OFFICE OF TECHNOLOGY | OFFICE OF INFORMATION SECURITY AND CONTROLS