ARE YOU HEADED FOR A DATA DISASTER?

BY WILLIAM E. OTT

If your EMS agency stores patient and response information in an electronic data system, it is highly likely that your data can be easily lost, stolen, or misused. If your data is contained on more than just a single, non-networked PC, the potential for loss or misappropriation of your data is exponentially larger.

The Health Insurance Portability and Accountability Act (HIPAA) is the largest legislative act ever that impacts health information security. Most EMS agencies will have to be HIPAA compliant by April 14, 2003. Non-compliance can result in significant fines; deliberate misuse of private health information can result in fines and jail time. HIPAA is going to force most EMS agencies to address the security related issues raised here. Hopefully you are already well down this path.

RISKS TO YOUR NETWORK AND DATA

Network Access:

Assigning network addressing information automatically via Dynamic Host Control Protocol (DHCP). This allows authorized and unauthorized users alike to simply plug into a local area network (LAN) port and be on the network. While this doesn't necessarily provide authentication to join the domain, the reasonably skilled hacker only needs to be on the network to capture all network traffic with a packet sniffer. This information can be carried away from your site to be analyzed. If the data traveling on your network isn't encrypted, everything transmitted and captured by the intruder is easily viewable.

If any of your network cables are exposed to view the data traveling on those cables can be intercepted and collected by a method known at magnetic induction. Network testing tools are available with this technology to allow Information Technology (IT) workers to troubleshoot network problems. These same tools can be used by hackers to capture all network traffic to allow analysis at a later time.

Rogue and non-secured wireless access points:

Wireless computer networking has really exploded the past two years. It is a great convenience to be able to take your wireless enabled notebook to the conference room for a meeting yet still be connected to the server. Most of the currently deployed devices are using the IEEE standard 802.11b. Security was never a major design factor for these devices and that is starting to catch up to people now. If you have a wireless access point you are broadcasting all of your network traffic. This information can be captured easily by 'wardrivers' that ride around with a wireless equipped notebook PC and simple antenna. The wardriver could be in the parking lot, or as far as two miles away. These access points pose a huge security threat if not properly controlled. Not only is your data at risk, cases are now occurring where 'spammers' are using non-secured wireless access points to send their bulk unsolicited mail. This spam then appears to have originated from your network. If you use wireless network equipment, and there are many valid uses, it is critical that you control access, times of use, and encrypt all traffic sent wirelessly. You also should use a tool like Netstumbler to shake out rogue access points.

Lack of proper Firewalling and Intrusion Detection:

Anyone or any agency that is permanently connected to the Internet needs to have a firewall in place. In the simplest of terms, the firewall protects your internal network from the outside world. The firewall is configured to allow only authorized actions or services to come in or go out. Good firewalls are capable of auditing all activity and generating logs of this activity. It is important to set your firewall in full audit mode and then to review those logs on a regular basis. It takes a little time to become comfortable reading the logs but in time you learn to understand what is normal so that when something unusual shows up you can pick it right out. Reading the firewall logs is the simplest form of intrusion detection. There are intrusion detection systems (IDS) that can be added to your network to give you robust protection and notification immediately of bizarre network events.

Virii and other malware:

Virii, Trojans, worms, and other types of malware are constantly floating around on the Internet and some have the ability to bring your network down. It is vital to maintain a proactive anti-virus program on your network and PCs. This means staying updated with the latest virus definitions that are available from your vendor. These are usually published weekly and daily in some cases when a new threat is uncovered. You must also have policy in place controlling downloads, introduction of software on disc or other media that could be contaminated. E-mail seems to be the biggest threat still for the introduction of malware to your network or PC. Remember to practice safe computing by not opening unsolicited web links, file attachments, etc.. The most likely source of infection is from a friend or colleague that is infected and unaware of it. If you receive a file or link from a friend that is unexpected, call or write to confirm what it is prior to opening it. Proper firewalling can also assist in stripping certain dangerous attachments from e-mail.

No verifiable data backups or contingency plans:

If you have a data system in place, you are living very dangerously if you do not have a verifiable backup system in place with backups stored offsite for safety. Contingency planning is also vital for mission critical networks and applications. How long would it take to get your system back online if the server were destroyed by fire or structural collapse? What if half of your networked PCs were stolen or damaged? Having pre-existing network contingency and business continuity plans in place is more important than ever in the post September 11 world.

Social Engineering:

Many times network resources and confidential data are simply handed over to the hacker willingly and unknowingly. The scenario could be someone allegedly calling from IT to try and correct 'some' network issue. The hacker simply reassures and talks the victim into revealing their username which usually isn't secret, but then get the victim to reveal their password which is secret while the hacker posing as an authorized IT person then uses this information to gain access to the network or server. Many schemes of this type are possible, also many cases of a hacker simply walking in and acting as if they are from IT or are a vender there to

take the PC to fix or add something. Would your office staff verify this, or would they let it happen?

Lack of Computer Policy:

It is quite important that you have a policy in place that is clearly understood and signed for by all personnel that covers appropriateness of use, security issues, plugging personal notebooks into the LAN, loading software on the LAN, etc... This policy must clearly define the penalties for non-compliance.

Obviously all topics can't be addressed in one article, but I wanted to put these issues on the table and give you some information you could take to your IT personnel and say 'where do we fit in this?'

Network and data security are major issues in the healthcare environment. I hope to explore various technical issues related to these topics that will be of use to the EMS community. I welcome your comments, criticisms, feedback, and ideas. You may contact me at weo@cpcstech.com

William Ott is president and chief consultant of CPCS Technologies, a NC-based technology consultancy providing services to the public safety, and defense communities. He's been involved in EMS since 1981, in field, education and administrative capacities.

William E. Ott

Digitally signed by William E. Ott
DN: CN = William E. Ott, O = VeriSign, Inc., OU = VeriSign Trust Network
Reason: I am the author of this document
Location: Cary, North Carolina
Date: 2003.08.31 16:16:26 -04'00'