Cybersecurity: *Protecting Yourself, Your Agency and Your Patients from Hackers and Data Breaches*

By Paul Trusty, MS, CISPP

Use of electronic patient care reporting (ePCR) systems to collect, use and exchange personal information about patients and patient encounters is growing more commonplace throughout EMS. The data can be used to improve operational and billing efficiencies, measure the effectiveness of treatments and ultimately improve patient care.

But collecting and exchanging data electronically also poses risks to patient privacy. As information flows from mobile devices to computers inside EMS agencies, and potentially from EMS to hospitals, insurers and other healthcare partners, the risk of data breaches and cybersecurity incidents rises.

As an example: On May 12, businesses and healthcare organizations around the world were hit by the WannaCry ransomware attack, which essentially locked all of the documents and images on computers, rendering them unusable. When infected computers were turned on, a red screen popped up with the words, "Oops, your files have been encrypted!" and demanded payments of $300 in online Bitcoin – later rising to $600 and destroying files if not paid in a week.

The attack, considered the biggest in history, caused significant disruptions across the globe. According to news reports, National Health Service facilities in the United Kingdom had to cancel appointments and surgeries and divert ambulances because hospitals could not access any patient records.

Variations of this attack, made possible through a tool released by a hacking group known as Shadow Brokers, are likely on the horizon. And as electronic data collection and sharing increases, EMS needs to take steps to protect their agencies and their patients from such attacks.

To accomplish this requires commitment at every level – from the architects of EMS software to agency supervisors who can develop protocols and educate staff about patient privacy best practices. Individual practitioners also play an important role. Their behavior and awareness of these issues are critical in preventing data breaches and computer viruses from spreading.

MAIN CAUSE OF BREACH, INCIDENTS INVOLVING 500+ HEALTH RECORDS, 2016

130
Unauthorized Access/Disclosure

113
Hacking/ IT incident

62
Theft

16
Loss

7
Improper Disposal

Source: U.S. Department of Health and Human Services

STEPS FOR SOFTWARE VENDORS AND EMS AGENCIES

WannaCry ransomware exploited an aging computer communications protocol and poor cybersecurity practices to gain its foothold and wreak havoc. Research conducted by the Australian Department of Defense concluded that 85% of threats like these can be prevented by following four cybersecurity best practices.

1 **Application "whitelisting,"** or allowing only pre-approved, tested and secure applications to be downloaded onto organization computer networks.

2 **Patch operating systems quickly.** A patch is used to update software or fix a security vulnerability. The makers of operating systems such as Windows, IOS and Android periodically issue patches. Ideally, operating system updates should be implemented network-wide within three days of release.

This is more resource intensive than most people realize. Patches may require testing prior to release and computer networks may not be usable when updates are deployed.

EMS should also strongly encourage vendors to stay current with the latest operating systems and operating system updates. In the case of the recent ransomware attack, Microsoft, the maker of Windows operating system, had issued a patch in March that could have prevented the virus from spreading as widely. But many organizations had not applied the updates in a timely manner, allowing the hackers to exploit the security flaw.

3 **Patch applications quickly.** Applications such as Java, Adobe Flash and Acrobat are widely used in EMS and across many industries. Applications should be updated within three days of the release of a patch. This is also a resource intensive endeavor, but well worth it.

EMS may also have EMS-specific applications running on their computer networks. EMS should encourage software vendors to implement a cybersecurity program that identifies and updates vulnerabilities in their software.

4 **Restrict administrative privileges.** When users have local admin rights, they have the ability to do what they want at their computer workstation – download any application, run any program or override IT's security measures. Computers that have users with local administrative privilege are quite possibly compromised.

Malware is everywhere. Even websites we trust everyday have attackers posting ads that are designed to deliver malware. There are also many sites that have been compromised and reconfigured to deliver malware to unsuspecting users. Eliminating local admin privilege prevents malware from taking control of the entire operating system and spreading throughout agency networks.

HEALTHCARE DATA IS A PRIME TARGET

Through our ePCR systems, we collect protected health information that is of great value to criminals. In 2015, the Identity Theft Resource Center's Data Breach Category Summary Report indicated that healthcare accounted for 78% of the breaches of personal information.

In 2016, there were over 16 million records exposed. (This was actually a major improvement from 2015, when over 113 million were exposed, according to the U.S. Department of Health and Human Services.)

A major reason healthcare records are of interest to hackers is for identify theft, particularly medical identity theft. Medical identity theft results from criminals stealing protected health information (PHI) and selling it for others to use. Stolen medical identities are being used to get prescription medications, surgeries, and other medical care. The victims find themselves responsible for medical bills, struggling to obtain medical care, or facing legal issues from the actions taken by those using their medical identities.

REASONS FOR SECURITY LAPSES

When cybersecurity incidents occur, there are many reasons why an organization may fail to protect the data they were trusted with. Software solutions have fallen behind, users grow weary of the lack of control over the computer they use, updates create problems and result in application downtime, and the frequency of third party updates overloads IT departments.

It is by no means a simple task to implement cybersecurity in an organization. It takes commitment from every level, and is ultimately the responsibility of the top executives, the board of directors, or the city council to require it.

An information security program should be implemented that at minimum includes a risk management component and employs mitigation strategies against identified risks. The program should then run just like every other quality improvement program – identifying and measuring risk, addressing it, and measuring again. Local cybersecurity companies can be used to create a baseline and a cybersecurity plan.

> *KnowBe4, which offers security awareness training for companies, has a free "hostage rescue manual" which provides guidance on warding off hackers and ransomware.*
>
> *https://www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf*

HOW EMS PRACTITIONERS CAN PROTECT THEMSELVES AND THEIR PATIENTS

So what can an individual practitioner do?

When it comes to mobile devices, using high quality passwords, remembering to log out and keeping a close eye on your mobile devices can prevent theft and prevent unauthorized access to patient information.

To protect against malware and ransomware, awareness is important. According to media reports, a group purporting to be the WannaCry hackers have claimed the ransomware was stolen from cyberspies that have worked with the U.S.'s National Security Agency. It all sounds terribly sophisticated.

But the primary method of infecting computers with ransomware starts by enticing individuals to click on or download infected attachments through phishing attacks, or spam emails. Another strategy uses emails that encourage users to click through to a website where malware resides.

A newer tactic is "malvertizing" – online ads containing malware on websites you trust. Ad blockers can help cut down on malicious ads. But anytime you're browsing the Internet, be careful with what you click on. If an email or a link looks suspect, delete it.

What is ransomware?

Malicious software that locks all documents, images and music on a device, such as a computer, tablet or smartphone and then demands a ransom to retrieve the files. If the ransom isn't paid (and sometimes even if it is), the files are destroyed.

How does ransomware infect a computer?

Typically, the virus is in an email attachment that, when opened, encrypts all data on the computer's hard drive, making it impossible to access.

How can you protect yourself?

Anti-virus software can protect your machine, although hackers are always developing new ways to circumvent such protections.

Paul Trusty is a paramedic, Certified Information Systems Security Professional and director of information security for Tarrant County College District in Texas.