Inform
Newsletter

All Clinical Informatics, Inc.

www.acinformatics.com 561-737-2267 May 2016

Avoiding Data Breaches and Ransomware Attacks

Your users are your biggest risk

The simple act of opening an email or clicking on a website link can allow a computer to be controlled by an outsider. They may try to steal your patient data for its value on the black market, or they may simply encrypt your data and hold it hostage, charging you a ransom for the key. Either way, this can lead to an expensive and damaging situation that is bad for your patients, bad for your reputation, and even bad for your cash flow if your data is inaccessible. **Some businesses don't survive this type of compromise**.

The 2015 Data Breach Investigations Report[1] from Verizon analyzes data breaches and their causes across industries. Despite the fact almost all breaches are from external attacks (85%), they found that inside users are often the conduit for these attacks, with almost 1 in 4 users failing to recognize a phishing email before they open it, and about half of those actually click on the malicious link or website contained in the email.

Unfortunately, email phishing attacks are becoming very convincing, as they mimic shipping labels, e-fax notifications, banking alerts and other messages that consumers have come to expect in their email. This makes user awareness and training ever more important as one of the front lines in your network security efforts.

Here are 4 things you can do at work and at home to minimize your risk:

1. Educate users on email and browser security. Teach best practices such as:

Don't open emails from senders you don't know or expect, or that look suspicious (misspelled or nonsensical Subject line or text, grammatical errors, email contains nothing but a link, etc).

Always hover over a link with your mouse to see the actual destination address of the link before you click. The destination usually displays in the lower left corner of the window (if you don't see it, turn on the View Status bar). If the domain name looks wrong, and especially if it is from another country (.ru or .cz instead of .com for example) it is very likely bad and the email should be deleted.

Don't read personal emails on work computers, especially from public mail services (like Gmail, Yahoo, Hotmail, etc.) to reduce your exposure to phishing attacks on the business network. Use a smartphone for reading emails or doing personal web surfing.

Be sure anti-malware protection and operating system patches are up-to-date on any computer you use for the Internet.

2. Limit access rights by Role to contain the damage from an infected user account or compromised computer.

[see Data Breaches, page 2]

How to Pick a Great Password

Almost all systems now require a complex password, and many of them want you to change that password regularly. However, you're usually blocked from using regular words found in the dictionary, and even adding a couple of numbers or punctuation to a regular word does not necessarily improve its security.

One method of constructing a hard-to-guess password is to pick a short phrase that is easy to remember, then build a password from the 1st letter of each word, plus punctuation and some creative replacement numbers. For example, the phrase "If it ain't broke, don't fix it!" could become the secure, complex password Ii8b,dfi!

Another easy trick is to use symbols to replace letters or numbers. Replacing the letter O with a number 0 is an obvious trade and included in most dictionary attacks, but replacing the letter O or number 0 with parenthesis () is not so obvious yet easy to remember. V's and W's can be replaced with \/ and \/\/ (a combination of forward and backslashes). X's can be replaced with >< (right and left arrows). You can get as creative as you want with this.

Once you have a great password that is easy to remember but hard to guess, you can survive future password changes by adding a sequence number or letter to make it different enough to use while still similar enough to recall.

Data Breaches from page 1

Use non-administrator accounts for all routine day-to-day activities on computers, even at home.

Restrict access based on job functions for each network user account, defining access rights specific to each job. Role-based access control assigns rights to groups, then adds users to groups.

3. Protect computers from malicious software

Use an operating system with current support, and set updates to apply automatically to fix new vulnerabilities as soon as they become known and patched.

Install a well-known antivirus package and run nightly full scans to clean anything missed by the real-time malware checker.

4. Back up your important data regularly

Run full backups periodically (monthly or quarterly).

Run differential backups more frequently (daily, hourly, prn) capturing all adds and changes since the last full backup.

Store backup media off-site. The backup is not complete until the media has left the building. Online backup services make this easy.

Backup personal data on your home PCs to an external USB drive, such as a WD Passport, then store that backup drive disconnected and away from the computer, to protect your data from theft or loss due to drive failure or malicious encryption.

*These 4 guidelines will **reduce your risk** dramatically, **limit your damage** in a successful attack, and ensure any loss of data is **fully recoverable**.*

Reference:

http://www.verizonenterprise.com/DBIR/2015/

CPC+ is coming for Primary Care

On April 11, CMS announced its largest-ever initiative to transform and improve how primary care is delivered and paid for in America. The **Comprehensive Primary Care Plus** (CPC+) model is designed to provide doctors the freedom to care for their patients the way they think will deliver the best outcomes, and to pay them for achieving results and improving care.

The Model

CPC+ is an advanced primary care medical home model that rewards value and quality by offering an innovative payment structure. The model will offer two tracks based on the current level of medical home capabilities at each practice (basic or advanced). Practices in both tracks will be expected to make improvements in the way they deliver care, centered on key Comprehensive Primary Care Functions:

(1) **Access and Continuity** – optimize continuity and timely, 24/7 access to care, as guided by the medical record.

(2) **Care Management** – Patients with serious or multiple medical conditions need extra support to ensure they are getting the medical care and/or medications they need.

(3) **Comprehensiveness and Coordination** - Primary care is the first point of contact for many patients, and takes the lead in coordinating care as the center of patients' experiences with medical care.

(4) **Patient and Caregiver Engagement** – engage patients and their families in decision-making in all aspects of care, including improvements in the system of care.

(5) **Planned Care and Population Health** - proactively assess patients to determine needs and provide appropriate and timely chronic and preventive care, including medication management and review. Develop a personalized plan of care for high-risk patients and use team-based approaches to meet patient needs efficiently.

The Benefits

Medicare will pay a monthly risk-adjusted care management fee averaging $15 per beneficiary in addition to regular fee-for-service payments, for Track 1 practices. Track 2 practices will average $28 per beneficiary, and some of that fee is paid as a lump sum at the beginning of the year as advance E&M reimbursement. The care management fee is intended to help practices defray their costs of creating new workflows, hiring care management staff, and developing new relationships necessary to coordinate care.

On top of this care management fee, CMS also offers a performance incentive of $2.50 or $4.00 per member per month, also paid up front, for practices that maintain expectations on utilization metrics and quality.

CPC+ will be implemented in up to 20 regions and can accommodate up to 5,000 practices, divided evenly into Track 1 and Track 2 practices. By July 2016 the regions will be published and interested practices in those regions can begin applying for participation in this program.

Reference: https://innovation.cms.gov/initiatives/Comprehensive-Primary-Care-Plus