Viruses and malware have been around for a very long time. One of the latest and biggest variants is ransomware. With ransomware, your PC is infected and your files are encrypted. Either you pay the ransom to get access to your files (or in some cases, your computer), or you format and reinstall and restore from backup. One of ransomware’s biggest problems is that once your files are encrypted, it is nearly impossible to unencrypt them within the ransom period - usually two weeks. Modern cryptographic techniques would require decades to decrypt via brute force.

In 2016, there is now a new problem - Ransomware-as-a-Service. In the past, ransomware authors would create and deploy their own malicious programs. Now, they have adopted the Software-as-a-Service model that is popular with legitimate software developers. With Ransomware-as-a-Service, the authors create easy-to-deploy programs, which are then downloaded and deployed by others. When a victim pays up, the original author receives a percentage of the ransom and the person who deployed it receives the rest. While it may not seem like a big change, it makes ransomware much more prevalent. One author can write the program and hand it off, and 50 people can deploy the same program.

The best defenses you can have against ransomware and other malware have not really changed. Antivirus software should be in place and kept up-to-date. Internet filtering can also help. Once ransomware has been identified, its IP address can be blocked very quickly. Programs like Malwarebytes have a place, in addition to traditional antivirus software. And, of course, a solid backup strategy is vital so that important files are not lost.

You can read more about Ransomware-as-a-Service by downloading Verisign’s 2016 Cyberthreats and Trends Report at http://tinyurl.com/zx5n3gi.
These are crazy high pressure times we live in. Throughout my career working in the mental health and addictions information technology (IT) world, I have never experienced anything like this. With the changeover to fee-for-service, agencies need to find ways to better service their community with less money and fewer resources. IT has an essential role in this.

As IT professionals, you need to provide the right tools for staff to get their jobs done as efficiently as possible. You need to provide access to systems and data while protecting the data from inside and outside threats. You need to help staff manage and interpret data to make fact-based decisions or bring resources that can assist with this. You need to know the best hardware, software and services that are available now. You need to understand your agency’s business and understand the big and ever expanding world of IT.

How can anyone keep up and know all this? You and I can’t; it simply is not possible. I am always concerned when someone claims to be an expert. Yes, they may know a lot more than me, but there is so much to know and there is always someone who knows more than the expert. Anyway, we all need to continue to seek information and learn more. To that end, if you have not taken advantage of the IT Project’s free workshop series, you should. We get speakers to present educational workshops on different subjects. Usually, presenters who are knowledge leaders work for companies that want to sell products or services. We ask them to present non-marketing educational workshops so you walk away with some new knowledge to help you do your jobs or assist your agencies. These workshops are held at our offices or at a facility nearby or presented on the web. The IT Project offers topics that are relevant to the community. We have had workshops on cyber security, disaster recovery planning, ICD-10 and HIPAA compliance and social media, as well as workshops on selecting, implementing and effectively using electronic health record software. There are so many; the list goes on and on.

My point in the end is: Please take advantage of these FREE workshops. Look for our e-mails and visit our webpage, http://njamhaa.org/free-trainings, to see what has been posted. There are four workshops in September. Let me know if you are not getting information about them and want to, so I can add you to our e-mail list. Please let me know if you have a topic you would like to see presented and I will try to make it happen. If you have a topic you would like to present, please contact me. I would like to set something up to meet your needs.

Take advantage of this free resource. Who knows? It may help make your job just a little bit easier.

Also, if you haven’t discovered our IT resources section on NJAMHAA’s website yet, please visit www.njamhaa.org/resources for a plethora of informative articles.

Regards,

Ron Gordon

Ron Gordon
Director, IT Project
RGordon@njamhaa.org
New Jersey Hospitals Are among the Nation’s Most Wired

By Amina Razanica, razanica@njha.com
Reprinted with permission

New Jersey hospitals are among the nation’s “Most Wired”. According to the July 5, 2016 edition of Hospitals & Health Networks magazine, 18 hospitals in New Jersey are named among the nation’s “Most Wired” hospitals, one was cited as a most improved hospital, and another received an Innovators Award. These annual awards are based on surveys from hospitals in the field, looking at areas such as electronic health records, telehealth, security and privacy.

The “Most-Wired” hospitals are leaders in cybersecurity, telehealth, security and analytics to improve quality and data management to reduce costs. Ninety-two percent use cybersecurity defensive measures such as intrusion detection systems. Sixty-seven percent are using pattern detection to prevent automated logins. Forty percent are performing risk assessments for social engineering, which uses personal interaction like phishing e-mails to workers to obtain password information or other protected data. Sixty-one percent use telemedicine for office visits and consultations. Eighty-four percent are using population health applications to identify and target patients for outreach, and 58 percent are synchronizing clinical and financial risk measures for clinical, operations and compliance standards.

New Jersey’s “Most Wired” hospitals and systems are:

- CentraState Healthcare System*
- Clara Maass Medical Center
- Englewood Hospital and Medical Center
- Hackensack University Medical Center
- Holy Name Medical Center
- Inspira Health Network (three hospitals)*
- JFK Medical Center*
- Meridian Health*
- Monmouth Medical Center*
- Monmouth Medical Center Southern Campus*
- Newark Beth Israel Medical Center
- Robert Wood Johnson University Hospital
- Robert Wood Johnson University Hospital Hamilton
- Robert Wood Johnson University Hospital Somerset
- Saint Barnabas Medical Center
- Trinitas Regional Medical Center*
- Valley Health System
- Virtua
- Cooper University Health Care

* NJAMHAA Members

New Jersey hospitals are among the nation’s “Most Wired”. According to the July 5, 2016 edition of Hospitals & Health Networks magazine, 18 hospitals in New Jersey are named among the nation’s “Most Wired” hospitals, one was cited as a most improved hospital, and another received an Innovators Award. These annual awards are based on surveys from hospitals in the field, looking at areas such as electronic health records, telehealth, security and privacy.

The “Most-Wired” hospitals are leaders in cybersecurity, telehealth, security and analytics to improve quality and data management to reduce costs. Ninety-two percent use cybersecurity defensive measures such as intrusion detection systems. Sixty-seven percent are using pattern detection to prevent automated logins. Forty percent are performing risk assessments for social engineering, which uses personal interaction like phishing e-mails to workers to obtain password information or other protected data. Sixty-one percent use telemedicine for office visits and consultations. Eighty-four percent are using population health applications to identify and target patients for outreach, and 58 percent are synchronizing clinical and financial risk measures for clinical, operations and compliance standards.

New Jersey’s “Most Wired” hospitals and systems are:

- CentraState Healthcare System*
- Clara Maass Medical Center
- Englewood Hospital and Medical Center
- Hackensack University Medical Center
- Holy Name Medical Center
- Inspira Health Network (three hospitals)*
- JFK Medical Center*
- Meridian Health*
- Monmouth Medical Center*
- Monmouth Medical Center Southern Campus*
- Newark Beth Israel Medical Center
- Robert Wood Johnson University Hospital
- Robert Wood Johnson University Hospital Hamilton
- Robert Wood Johnson University Hospital Somerset
- Saint Barnabas Medical Center
- Trinitas Regional Medical Center*
- Valley Health System
- Virtua
- Cooper University Health Care

* NJAMHAA Members
Healthcare Data Breaches Are a Source of Concern

There have been many sleepless nights as healthcare Chief Information Officers and Chief Information Security Officers toss and turn, often waking up in cold sweat, their breath caught in their chests as one phrase pinballs through their brains: Security Breach. In this technological climate, when everything is electronically available and technology is growing faster than the average worker can learn, diligence and education are keys to survival. Do not think that this is something that will only happen to somebody else, because we are all somebody else to somebody else.

Not even healthcare giants like Anthem, who is the second largest payer in the world, are exempt from breaches of security. In fact, the largest healthcare breach ever reported occurred in 2015 when Anthem reported that 78.8 million patient records were compromised. Furthermore, of the five largest breaches to happen in 2015, four of them happened to healthcare organizations that employ state-of-the-art tools designed to stop these very breaches from happening. It’s not a software issue; it’s not a technical issue. The issue, quite simply, is people. In almost every incident, an employee fell for a phishing e-mail that enticed them to do something to put their organization at risk. And yes, even high-level information technology executives got hooked and pulled in.

So, why is healthcare so valuable? Information can be sold on the black market and each piece of personal identifiable information (PII) has its own perceived value relative to a specific purpose. In one patient record, there is a total of 17 different combinations of PII, which renders healthcare data up to 10-20 times more valuable on the black market than standard stolen identity information. It’s a veritable gold mine for a hacker.

Fortunately for at-risk patients, but not organizations, hackers seem to be focusing less on stealing identities and more on ransomware attacks in which they will encrypt the information and charge a fee. They have done their homework on healthcare and know that a large hospital or health system with many employees in their workforce is a ripe target for taking their bait. The hackers have figured out they can get a higher payoff with less effort if they hack a large payer organization, but that’s not saying provider organizations are safe. In any case, diligence is required and security is of utmost importance. As threats continue to evolve, so does our need for situational awareness.

Conventional wisdom and HIPAA security rules recommended “data at rest” encryption as an important breach safeguard. Now we know that hackers will use ransomware to take control and encrypt even encrypted data, rendering it useless unless the organization pays the bitcoin ransom.

Early detection provides you with the opportunity to thwart the attack, but once your files are encrypted, there is little you can do. In fact, it has been unofficially reported that the FBI has suggested to just pay the ransom on the attacks since there really is no ability to prosecute and bitcoin is untraceable. The only offense, in this case, is a good defense. Protecting your company with reliable software and educating your staff on the very real dangers that are out there, will go a long way in preventing a cyber attack on your company.
Most people use Microsoft Outlook to check their mail. It works well with Microsoft Exchange. One program handles your e-mail, calendar and contacts. It’s been around on desktops for 20 years. Now, you can have Microsoft Outlook on your phone as well, for iOS or Android. The price is hard to beat – it’s free!

There are plenty of e-mail clients out there. Why should you consider Outlook? It has a few compelling features. If you’re using a personally owned phone and don’t want your work contacts in your phone contacts, you can have Outlook keep them separate. Outlook contacts and calendar events are confined to Outlook, rather than available to the entire phone. This also means that another calendar app will not be able to access your Exchange calendar.

Outlook also has two inboxes for mail – “Focused” and “Other”. “Focused” is mail sent to you by another person. It’s generally the “real” e-mail you get from co-workers and clients. “Other” is the mailing lists, alerts that we all subscribe to, but aren’t as important. It also includes plain old spam. Outlook is very good at distinguishing which is which, and if it gets it wrong, you can correct it and it will remember your correction. With this feature, you can go through your important e-mail first and save the alerts and mailing lists for later.

Also, Outlook can connect to several Cloud storage providers right in the app. If you’re using Office 365, all your e-mailed file attachments are in OneDrive for Business. Outlook can access it easily. That’s not its only trick, though: It can also connect to Dropbox, Google Drive, Box and several others.

Most of us just use the mail client that came on the phone, and that generally does a decent job of getting your e-mail. Outlook does a lot more. It’s worth a look.
USB Storage Grows Along with the Need to Protect your Data

Do you remember when you got your first thumb drive? 128 MB on a little chip! Suddenly, the need for a huge case of floppy disks went away. That was 12 years ago. In the time since then, we have seen an increase in the size of applications and hard drives. The thumb drive needed to keep up. Even the 1 GB drive has become too small. We have seen the drive increase in recent years to 8, 64 and even 256 GB’s.

The IT Project recently received a 2 TB thumb drive. Yes! That was not a typo! Two terabytes on a thumb drive! It is no bigger than any other drive. And it contains that much storage.

Most portions of our servers cannot store that much data. “Amazing!” you say.

Yes, but it brings up some very important questions about how to protect your data from loss, which, as we know, is a major HIPAA requirement, when someone can walk in with a little flash drive no bigger than a keychain and copy all the data on your network.

Blocking Access

The first security strategy is to eliminate access to these devices altogether. Microsoft Active Directory has ways that can help you with this.

First, the requirements: Your domain schema needs to be at 2008 or higher, and the workstations need to be at Windows Vista or above. Since, at this writing, the lower versions of the software, Windows 2003 server and Windows XP are out of service life, we should all meet this requirement. So, how can we secure the drives? The answer is through the use of Group Policies.

Group Policies, or GPO’s as they are known, are a powerful tool built into Windows that can control many things on PC’s and networks. GPO’s are broken down into two sections: computers and users. This means that specific rights can be applied to either a user or a computer.

This is how you will use it to secure flash drives:

The first step is to create an Organizational Unit (OU) in the active directory. Then, add the users or computers that you want to control that OU. You do this in ADUC (Active Directory Users and Computers). After this, you go to the Group Policy Manager and right click on the OU created and add a policy. You now need to edit the policy created and browse to one of the following keys, depending on if you want to use computer or user policies. If you utilize user policies, you can have different policies for different people. This means you can allow yourself to have one access and allow a standard user to have different access.


Inside this Policy are multiple choices on what to allow, as hinted at earlier. One choice is to block all access to the thumb drive. As this implies, all USB media will not function when inserted into the computer. A second choice is to allow read access to the drive; this is useful if your users occasionally work from home and carry the data on a flash drive. A third choice is to deny read access. The final policy is only available in per-computer policies and that is to deny execute. This will block the running of programs from a removable drive.

Encryption

The next consideration in using these flash drives is data security on the device. If you have decided that you want people to have the flexibility to use devices, you will need to protect the data the same as if it was on your network or a laptop hard drive; this means encryption and password protection. Much has been written in these pages about encryption, but it is such an important topic, we will briefly describe it. Encryption is a way of writing data so that only the intended person or persons have access to it. You can now purchase a flash drive that has built-in encryption. PC World magazine has reviews of some of the devices on pcworld.com

If you have a thumb drive that does not have built-in security, there are still choices for you. The first is Bitlocker, the encryption software that comes with Windows 7 Enterprise and Windows 10. You can use that to encrypt the drive. If you do not have the version of the software that has encryption, you can get third-party software. In the past, we recommended a program called TrueCrypt. Sadly, that program is not being updated any longer; however, it is still a good choice. Another choice is DiskCryptor, which can be used to encrypt drives and folders on drives. These are just two of the security choices available to use with these devices, but it should give you a good starting point to look.

So, as we can see, these new larger devices are very flexible. We admins must, therefore, adapt to the changing times and protect the data that is the real value on our computer systems. We need to encrypt, scan for viruses and, where applicable, block access to flash drives.
Ten Steps to Repair a Failing Profile in Windows 7

If you receive a “The User Profile Service failed the logon” error message when attempting to log in on a Windows 7 computer, you may be able to resolve the issue with the following steps:

It is always a good idea to back up your data when using the registry editor or working on user profiles.

1. Click Start and type regedit in the Search box; then press Enter.

2. In the Registry Editor, locate and select the following registry subkey:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

3. Locate the folder that begins with S-1-5 followed by a long number.

4. Select each S-1-5 folder until you locate the one that contains the path of the profile having the error.

5. If you have two folders starting with S-1-5 followed by some long numbers and one of them ended with .bak, you have to rename the .bak folder. To do this, follow these steps:
   - Right-click the folder without .bak, and then click Rename. Type .ba, and then press Enter.
   - Right-click the folder that is named .bak, and then click Rename. Remove .bak at the end of the folder name, and then press Enter.
   - Right-click the folder that is named .ba, and then click Rename. Change the .ba to .bak at the end of the folder name, and then press Enter.

If you have only one folder starting with S-1-5 that is followed by long numbers and ends with .bak, right-click the folder, and then click Rename. Remove .bak at the end of the folder name, and then press ENTER.

6. Click the folder without .bak in the details pane, double-click RefCount, type 0, and then click OK.

7. Click the folder without .bak, in the details pane, double-click State, type 0, and then click OK.

8. Close the Registry Editor.

9. Restart the computer.

10. Log into the account in question.
Ever since Windows 95, computer problems have often been solved by booting into Safe Mode. Safe Mode is a very basic operating mode that loads only the absolute minimum drivers necessary to start Windows. Programs that ran at startup don’t do so in Safe Mode; they’re just the basics. Your icons are huge, your color scheme may look strange, and you can’t get on the Internet, but if Safe Mode works, you know the problem is not Windows itself. Safe Mode is a common first step for addressing computer problems and has gotten countless PCs up and running, whether the problem was a virus or a program that just didn’t work right.

For many years and several versions of Windows, all you had to do to enter Safe Mode was tap F8 before Windows started. You’d be presented with a black and white menu and could choose Safe Mode or Safe Mode with Networking. Windows 10 does not support pressing F8. It boots up much faster than older versions of Windows – too fast to get that F8 tap in if you have an SSD and a modern UEFI BIOS.

So, how can you get into Safe Mode?

There are four ways:

The first is to boot normally into Windows and use MSCONFIG. MSCONFIG has been around for a very long time and allows you to tweak programs that run at startup, as well as in other settings. Even if your machine is sluggish, you may be able to get into Windows. Type “System Configuration Utility” into the search bar and click on “System Configuration Utility” when it comes up. Pick the “Boot” tab (the second tab). Check “Safe Mode” and click “Minimal”. When you click “OK”, MSCONFIG will tell you it has to restart to apply the new settings, and when you reboot, you’ll be in Safe Mode.

The second way is to use the Shift-Restart combination. Click the start button and hold down the shift key. While holding that, click “Power” and then “Restart”. Rather than booting into normal Windows, you will be offered a menu with three options: “Continue”, “Troubleshoot” and “Turn Off your PC”. Select “Troubleshoot”. Now, you’ll get another menu choice of “Reset this PC” or “Advanced Options”. Choose “Advanced Options”. Another menu will come up with choices for “System Restore”, “System Image Recovery”, “Startup Repair”, “Command Prompt”, “Startup Settings” and “Go Back to the Previous Build”. Choose “Startup Settings”. You’ll have to reboot, but now, you can enable Safe Mode and Safe Mode with Networking by pressing F4 or F5.

The third way is to create a recovery drive. Windows 10 includes the Recovery Drive app, which will allow you to make a USB flash drive into a recovery drive that you can use to boot your computer. You’ll have the same troubleshooting options as you would have in the second method. This may be the only option if your PC will not boot into Windows at all. However, you have to have created the USB recovery drive before you started having problems.

The fourth way is the good old-fashioned F8 tap, but, in order to use this, your computer cannot have a UEFI BIOS (which most modern PC’s do) or an SSD (which aren’t quite as common). If your PC is an older model that was upgraded to Windows 10, it might work. As time goes by and more PC’s come out, this method will become less and less likely to work.