HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc.
Serving Roanoke and surrounding areas since 2006
757-333-3299 x232

February 15, 2015

Volume 1, Issue 1

ANTHEM LOSES DATA ON 80 MILLION

Anthem, Inc. reported week before last that hackers had stolen the data of approximately 80 million of its subscribers. Because the data was in their databases and not in an EHR (Electronic Health Record) it was not required by law to be encrypted. This does not appear to be a breach of treatment information, but, a breach of ***personal information***. What is the difference? To the Criminals behind these intrusions, a lot. They don't care whether you have gout or a bad heart. What they want is your name, Social Security number, and date of birth. Because with those key pieces of information, they can steal your identity. And, with a stolen identity, then can open up new credit cards, new bank accounts, take out loans, buy homes and cars, travel and never pay the bill…because **YOUR** name is on the bill.

Whether you are a Physician's Office or not, your business records might contain similar information. This information contained from the stolen medical record sells for $50 - $100 for each record on the Internet. By comparison, a credit card is worth about $1 on the Internet? Why? Because a credit card is worthless as soon as you report it missing, which means its shelf life is generally measured in hours. Your personal information never expires or goes stale. Even if you go to court and change your name, you still cannot change your birthdate or change your Social Security number.

6 Ways To Protect Yourself

1. Get a password manager program and use it
2. Stop reusing passwords and user IDs
3. Don't click on ANY link in an email that you are not 100% sure of (that is almost all of them)
4. Review credit card and Bank Statement often (at least weekly)
5. Check your credit reports
6. Put a 90 day Fraud Alert or Security Freeze on your account. There are 3 repositories of credit information: Experian, Trans Union and Equifax. Contact ALL of them.

SECURITY, SECURITY, SECURITY

SONY, HOME DEPOT, JPMORGAN, EBAY, TARGET, ADOBE, CITIGROUP, DSW SHOES. WHAT DO THEY HAVE IN COMMON? THEY ALL LOST CUSTOMER DATA TO HACKERS.

PEOPLE, THIS IS A NEW BALLGAME. THIS IS A NEW WAY OF DOING BUSINESS, THE WORLD HAS CHANGED. THE INTERNET IS LIKE THE WILD WEST OF YEARS GONE BY. WAKE UP AND PAY ATTENTION. **YOUR BUSINESS DATA IS AT RISK.** CRIMINALS NO LONGER HAVE TO STEAL A GUN AND ROB A BANK TO GET MONEY. THEY CAN SIT AT HOME IN THEIR UNDERWEAR AND STEAL WITHOUT EVER LEAVING THE HOUSE.

YOUR BUSINESS NEEDS TO DEVELOP A **CULTURE OF SECURITY** IN ORDER TO PROTECT THAT BUSINESS AND YOUR CUSTOMERS. IF THIS IS TOO "BIG-BROTHERISH" FOR YOU, THEN YOUR ONLY CHOICE IS TO DISCONNECT FROM THE INTERNET, THROW AWAY ALL THE COMPUTERS, AND BUY A LOT OF PAPER AND

HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc. February 15, 2015 Volume 1, Issue 1
Serving Roanoke and surrounding areas since 2006
757-333-3299 x232

some #2 pencils and go back to doing it "old-school". If that is not a choice, then read on….

A Culture of Security begins with a Risk Analysis of your current network environment. Physician's offices were required to begin conducting Risk Assessments in 2005. For other businesses, the same Risk Analysis done for a Physician's office, will also work in your environment/business. The key is performing an independent audit of your computer network security by someone who is not afraid to say, "The Emperor has no clothes".

The ability to perform a Risk Analysis/Assessment is a talent that requires the mindset not unlike a Police detective. All aspects of the computer networks along with the actual business operations must be open to scrutiny. The end goal is to find any place that data may have a chance of leaking out of the business and eliminate as many of those potential leaks as possible. For the rest, steps are taken to minimize the risk to a level acceptable to management in conjunction with compliance with governmental regulations.

This process is a pain.

But, this process is not negotiable. For medical offices, the HIPAA Security Rule dictates that you **will** perform a Risk Analysis and that you **will** remediate the problems found and that you **will** update the Risk Analysis on a regular basis. Period. End of story. No further discussion.

The government has stuck their nose further into the Physician's office with HIPAA and with that involvement come certain new laws and regulations. You may have been able to ignore those laws and regulations for a the past few years, but, rest assured that given all of the huge data breaches lately, you will not be able to keep your head stuck in the sand much longer.

You might as well begin treating HIPAA compliance in the same manner and with the same deference that you give the Internal Revenue Service. Because the folks at HHS (Health and Human Services) charged with enforcement have the ability to hurt your pocketbook and send you to jail, just like the IRS.

So, now is the time to add a budget item for your security and compliance program, and budget for an outsourced IT company to oversee that program. Before you ask, the answer is "no". You and your staff have too many things on your plate now and you cannot do this yourself. If you try, you will fail to complete it successfully which puts the business at risk for huge fines from HHS and the OCR (Office of Civil Rights). The typical Practice Administrator or staff person is not computer savvy enough to know what to look for and where to look for all of the potential points of data leakage. And, even if you found all of them, do you have the tools at your disposal to treat them properly?

Look at it this way. I come to your medical office because I have a problem. You examine me and pick a course of treatment. If you cannot figure it out, you send me off to a specialist for a diagnosis and treatment. This process is the same. You have an Accountant because you do not know the tax laws, you have an Attorney because you do not know all of the state and federal laws.

Computers and network security have gotten too complex in the past few years for a "part-timer" to keep up with. I think that it is great that your sister's nephew's son's cousin's child has been able to take care of your businesses computer needs after school every day. But, times have changed and unless that person is keeping up with the constant, ongoing, never ending changes in the computer business, then even a small office has outgrown that person's abilities. Today's typical business relies on computers and the Internet. So, what used to work for computer service, generally doesn't work any longer. If all of the data breaches have you even the least bit concerned, then it is time to bring in the pros for a Risk Analysis so you can get started fixing the problems that **you know you have.**

HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc.
Serving Roanoke and surrounding areas since 2006
757-333-3299 x232

February 15, 2015

Volume 1, Issue 1

PHISHING IN THE WAKE OF ANTHEM BREACH

Phishers and phone fraudsters are capitalizing on public concern over a massive data breach announced this week at health insurance provider **Anthem** in a bid to steal financial and personal data from consumers.

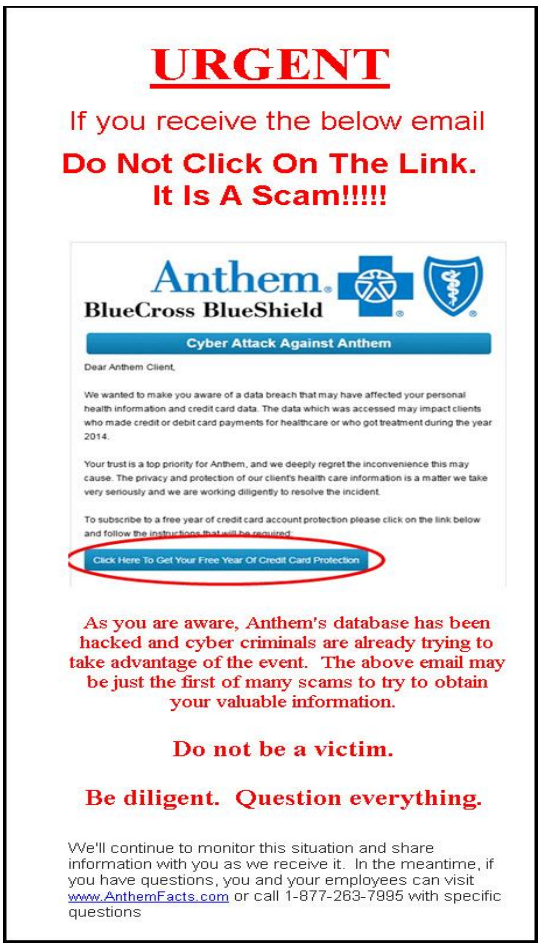
The flood of phishing scams was unleashed just hours after Anthem announced publicly that a "very sophisticated cyberattack" on its systems had compromised the Social Security information and other personal details on some 80 million Americans.

In a question on its FAQ page about whether it would be offering credit monitoring to affected customers, "Anthem said all impacted members will receive notice via mail which will advise them of the protections being offered to them as well as any next steps." Unsurprisingly, phishers took that as an invitation to blast out variations on the scam pictured below, which spoofs Anthem and offers recipients a free year's worth of credit monitoring services for those who click the embedded link.

Don't click or respond to these phishing emails.

According to Anthem, fraudsters also are busy perpetrating similar scams by cold-calling people via telephone. In a recording posted to its toll-free hotline for this breach (**877-263-7995**), Anthem said it is aware of outbound call scams targeting current and former Anthem members.

"These emails and calls are not from anthem and no notifications have been sent from anthem since the initial notification on Feb. 4, 2015," Anthem said in a voice recording on the hotline.



URGENT

If you receive the below email

Do Not Click On The Link. It Is A Scam!!!!!

Anthem BlueCross BlueShield

Cyber Attack Against Anthem

Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our client's health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required.

Click Here To Get Your Free Year Of Credit Card Protection

As you are aware, Anthem's database has been hacked and cyber criminals are already trying to take advantage of the event. The above email may be just the first of many scams to try to obtain your valuable information.

Do not be a victim.

Be diligent. Question everything.

We'll continue to monitor this situation and share information with you as we receive it. In the meantime, if you have questions, you and your employees can visit www.AnthemFacts.com or call 1-877-263-7995 with specific questions

This information is provided as an educational service by Computer Networks, Inc. For more information about our company and how we can help you, please visit our website:

www.computernetworksinc.com

HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc.
Serving Roanoke and surrounding areas since 2006
757-333-3299 x232

February 15, 2015

Volume 1, Issue 1

ONC Calls for Interoperability by 2017

So, the Office of the National Coordinator released a draft roadmap, along with proposed actions to take in order to achieve interoperability between EHR systems in the next two years.

The document, ***Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap Draft Version 1.0*** outlines steps "that will enable a majority of individuals and providers across the care continuum to send, receive, find and use a common set of electronic clinical information at the nationwide level by the end of 2017."

The "time has come for us to be more explicit about standards," said ONC Chief Karen DeSalvo, MD, in a Jan. 30 press call detailing the roadmap, a 150-page plus document addressing everything from governance, standards and certification to privacy and security. "Health IT that facilitates the secure, efficient and effective sharing and use of electronic health information when and where it is needed is essential to better care, smarter spending and a healthier nation," DeSalvo said.

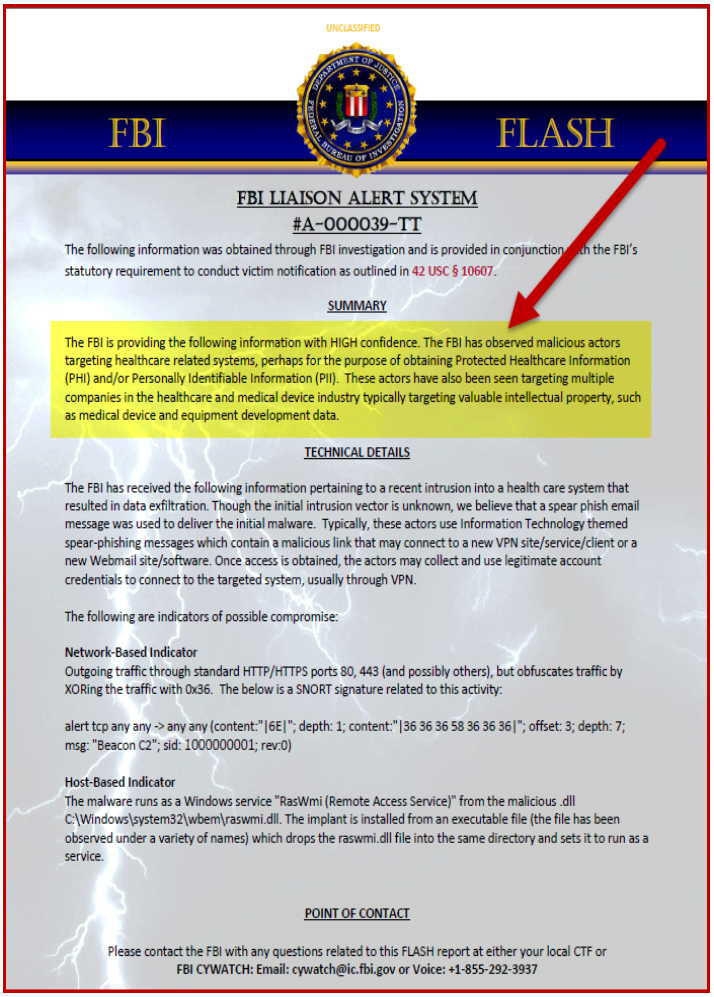
ONC is accepting public comments and key commitments on the draft Roadmap for approximately 60 days, which will end at 5 p.m. ET on April 3, 2015.

In her letter at the start of the roadmap, DeSalvo emphasizes that several action steps will be needed on the road to interoperability. The works, she writes, will occur along three critical pathways:

1. Requiring standards;
2. Motivating the use of those standards through appropriate incentives; and
3. Creating a trusted environment for the collecting, sharing and using of electronic health information

On the privacy and security front, the roadmap calls for "additional education" to educate stakeholders that have been misinformed about HIPAA and federal data privacy laws.

FBI ALERT



UNCLASSIFIED

FBI FLASH

FBI LIAISON ALERT SYSTEM
#A-000039-TT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

SUMMARY

The FBI is providing the following information with HIGH confidence. The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

TECHNICAL DETAILS

The FBI has received the following information pertaining to a recent intrusion into a health care system that resulted in data exfiltration. Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware. Typically, these actors use Information Technology themed spear-phishing messages which contain a malicious link that may connect to a new VPN site/service/client or a new Webmail site/software. Once access is obtained, the actors may collect and use legitimate account credentials to connect to the targeted system, usually through VPN.

The following are indicators of possible compromise:

Network-Based Indicator
Outgoing traffic through standard HTTP/HTTPS ports 80, 443 (and possibly others), but obfuscates traffic by XORing the traffic with 0x36. The below is a SNORT signature related to this activity:

alert tcp any any -> any any (content:"|6E|"; depth: 1; content:"|36 36 36 58 36 36 36|"; offset: 3; depth: 7; msg: "Beacon C2"; sid: 1000000001; rev:0)

Host-Based Indicator
The malware runs as a Windows service "RasWmi (Remote Access Service)" from the malicious .dll C:\Windows\system32\wbem\raswmi.dll. The implant is installed from an executable file (the file has been observed under a variety of names) which drops the raswmi.dll file into the same directory and sets it to run as a service.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at either your local CTF or
FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937

I don't think I can say it any better than the FBI…

Regulatory Compliance is a Natural by-product of Good Security