HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

July 15, 2015

Volume 1, Issue 7

KLAS Research
Blogs | From the Research Desk |

1,217 PHI Breaches and Counting

by Austin Cameron on May 27, 2015

Since October 2009, 1,217 breaches of unsecured protected health information (PHI), each affecting more than 500 individuals, have been reported to the Office for Civil Rights. These breaches have affected a total of 133,253,121 people. As smaller breaches do not need to be reported to the U.S. Department of Health and Human Services, the real number of PHI breaches is certainly much higher. For instance, the Identity Theft Resource Center (ITRC) has found that since 2005, breaches in the medical/healthcare industry have affected more than 156 million people.

The frequency with which hackers are targeting the healthcare industry is exploding. **Cyber attacks on healthcare companies increased 72% between 2013 and 2014, and ransomware attacks (blocking system access until $$ is paid) soared 113%.** Digital invasions into hospital data increased 600% in only 10 months in 2014, and **during the first 4 months of 2015, more than one-third of all data security breaches tracked by ITRC came from medical/healthcare companies.**

This onslaught is fueled by the skyrocketing value of PHI on the black market. Earlier this year, one hacker was found selling a "value pack" of 10 people's Medicare numbers for the equivalent of $4,700. The multiple avenues available to exploit PHI, combined with the extreme difficulty of preventing the misuse of medical information once its security has been breached, are why Eva Velasquez, president of the ITRC, refers to the healthcare industry as playing a game of Whack-A-Mole.

Needless to say, most providers my colleagues and I have spoken with about data security are feeling overwhelmed, unsure of where their vulnerabilities lie, and sometimes completely lost as to what to do or who to go to for help.

IT CAN'T HAPPEN TO ME

It can happen to you!

The Client in the message below is not a huge Practice and was not "targeted" by the criminals.

Zero Day Infections

Last week a staff member at a Client's office downloaded some malicious software off the Internet. The software turned out to be a variant of CryptoLocker that was not detectable by the local Kaspersky antivirus agents we have installed on the Client's network because it was too new.

However, the infection was picked up by the 11:00pm nightly Kaspersky deep scan which uses a different technology to look for malicious items. We got rid of the problem, but the damage was already done.

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

July 15, 2015

Volume 1, Issue 7

For the uninitiated, CryptoLocker silently begins to encrypt all of your files in the background without showing evidence that it is there. Once it encrypts your local PC files, it moves to any network drives that you have and encrypts the files on the server.

You are unable to open encrypted files without a key. The criminals offer to sell you the key, which is reported to sometimes work and sometimes not work.

In order to recover, we had to restore the Client's files from two days prior (the previous days tape was not available because it was with a staff member) which means that the Practice had to recreate two + days of data/appointments/correspondence/transcription, etc.

Lessons to be learned/takeaways-

1. **Educate your staff on proper Internet usage**
2. **Install a UTM (Unified Threat Management firewall) device that has the ability to detect some of these types of infections/behaviors**
3. **Restrict staff usage of the Internet by using a UTM device**
4. **Install a more sophisticated Backup than tape (our Disaster Recovery appliance would have allowed a recovery of less than 59 minutes) Which means that a maximum of 59 minutes of data would have to be recreated-not two + days worth of data**

Regulatory Compliance is a Natural by-product of Good Security

Healthcare Adjusts To Life As Hacker Target

Posted on Jul 01, 2015
By Mike Miliard, Editor

During the Cold War, back when Richard "Dickie" George was a mathematician at the National Security Agency, security meant something different than it does today. The foes knew one another well. And if there was plenty of skullduggery to go around, at least there were some recognizable rules of engagement.

"Back when it was us and the Soviets, there was about one big espionage event every 10 years," he said, speaking at the Healthcare IT News Privacy & Security Forum in Chicago on Tuesday.

In the 21st Century, the threat landscape is very, very different, said George, now a senior advisor for cybersecurity at Johns Hopkins University Applied Physics Lab.

To wit: There were more than 41,000 cyberattacks on government agencies in 2010 alone. That number has only risen. And the malefactors are only getting more insidiously creative.

"They just caught a refrigerator sending out 100,000 phishing emails," said George. "A refrigerator! It's a different world."

A different world, and a dangerous one. That was the theme that emerged – and was driven home again and again – at the Privacy & Security Forum.

Healthcare, especially, is at risk: Medical data is the number one aim for hackers and medical devices are loaded with potentially fatally-exploitable malware, said George, whose talk's

title – "Healthcare's Brave New World: Life as a Target" – said it all.

At Johns Hopkins, the challenge is acute and complex, he said: A network of hospitals, with the need to share information constantly. Add in myriad affiliated physicians practices of various shapes and sizes. And the fact that it's a large research university, with scores of students, many of whom are foreign nationals, with access to very sensitive health data.

"Risk management is really hard," said George.

Unfortunately, nowadays "everything you do is a risk management decision," he said. Because in an interconnected healthcare ecosystem, risk is omnipresent.

If you start with 1 percent good behavior and 99 percent bad behavior, and then work hard to improve that to 99 good behavior and 1 percent bad, you still haven't improved your security, said George. That 1 percent is still enough to pose serious security risk.

"People write code," he said. "People make mistakes. Security is never going to be perfect. People are going to get in."

Indeed, hackers' "creativity is shocking in some cases," said Dan Bowden, chief information security officer at University of Utah Health Care.

Bowden says he's seen an uptick in aggressiveness and ingenuity recently, with phishing and zero day attacks sharing more and more in common – almost becoming synonymous in some cases.

That necessitates an "endless cycle of discussion" reassessing data policies, IT strategies and vendor relationships, he said.

(One tip for those looking for business association with smart security strategies, he added: any time a vendor touts the fact that its "HIPAA-compliant," that should be "one of the biggest red flags." It speaks to a fundamental misunderstanding of what strong security requires.)

The threat is so omnipresent – and potentially so ruinously expensive – that many providers are increasingly turning to cyber insurance as risk mitigation strategy, said Erin Whaley, an attorney with Richmond, Virginia-based Troutman Sanders.

Such investments can indeed help defray a host of costs associated with a breach – hefty patient notification costs, fines, money spent hiring PR to restore damaged reputations, even funds to pay blackmail threats from ransomware, she said.

It's important, however, to tailor coverage levels to one's own organizational needs, adjusting according to gaps and vulnerabilities.

"If you've seen one cyber policy, you've seen one cyber policy," said Whaley.

In fact, "you may need layers of coverage to get to limits that make you feel comfortable," she said. "Even then, it may not cover all the costs associated with a breach."

One certainty exists, however: "Good insurance doesn't replace good security," said Whaley. "Good security is a prerequisite."

Insurers won't underwrite policies without demonstrably robust security practices, she said, since the payouts associated with healthcare data breaches are so huge.

Source URL:
http://www.healthcareitnews.com/news/healthcare-adjusts-life-hacker-target

HIPAA SECURITY BRIEF

By Computer Networks, Inc. July 15, 2015 Volume 1, Issue 7
Serving Hampton Roads since 2004

Phase 2 HIPAA Audits Kick Off With Random Surveys

By: Katherine Rourke

Ideally, the only reason you would know about the following is due to scribes such as myself — but for the record, the HHS Office for Civil Rights has sent out a bunch of pre-audit screening surveys to covered entities. Once it gets responses, it will do a Phase 2 audit not only of covered entities but also business associates, so things should get heated.

While these take the form of Meaningful Use audits, covering incentives paid from January 1, 2011 through June 30, 2014, it's really more about checking how well you protect ePHI.

This effort is a drive to be sure that providers and BAs are complying with the HIPAA privacy, security and breach notification requirements. Apparently OCR found, during Phase 1 pilot audits in 2011 and 2012, that there was "pervasive non-compliance" with regs designed to safeguard protected health information, the *National Law Review* reports.

However, these audits aren't targeting the "bad guys." Selection for the audits is random, according to HHS Office of the Inspector General.

So if you get one of the dreaded pre-screening letters, how should you respond? According a thoughtful blog post by Maryanne Lambert for CureMD, auditors will be focused on the following areas:

- *Risk Assessment audits and reports*
- *EHR security plan*
- *Organizational chart*
- *Network diagram*
- *EHR web sites and patient portals*
- *Policies and procedures*
- *System inventory*
- *Tools to perform vulnerability scans*
- *Central log and event reports*
- *EHR system users list*
- *Contractors supporting the EHR and network perimeter devices.*

According to Lambert, the feds will want to talk to the person primarily responsible for each of these areas, a process which could quickly devolve into a disaster if those people aren't prepared. She recommends that if you're selected for an audit, you run through a mock audit ahead of time to make sure these staff members can answer questions about how well policies and processed are followed.

Not that anyone would take the presence of HHS on their premises lightly, but it's worth bearing in mind that a stumble in one corner of your operation could have widespread consequences. Lambert notes that in addition to defending your security precautions, you have to make sure that all parts of your organization are in line:

> *Be mindful while planning for this audit as deficiencies identified for one physician in a physician group or one hospital within a multi-hospital system, may apply to the other physicians and hospitals using the same EHR system and/or implementing meaningful use in the same way. Thus, the incentive payments at risk in this audit may be greater than the payments to the particular provider being audited.*

But as she points out, there is one possible benefit to being audited. If you prepare well, it might save you not only trouble with HHS but possibly lawsuits for breaches of information. Hey, everything has some kind of silver lining, right?

A **Security Risk Analysis** is *required* for compliance. Call us today if you have not done yours or have questions about the process.

Rick Boyles
757-333-3299 x200
rick.boyles@computernetworksinc.com