HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

May 20, 2015

Volume 1, Issue 5

FBI: Health care related cyber crime expected to increase amid shift to electronic records

Cyber criminals are expected to step up attacks on health care system and medical devices, according to an FBI alert.

"Cyber actors will likely increase cyber intrusions against health care systems — to include medical devices — due to mandatory transition from paper to electronic health records, lax cybersecurity standards, and a higher financial payout for medical records in the black market," the FBI stated in a notice to industry dated April 17.

The combination is "generating a rich new environment for cyber criminals to exploit," the FBI stated, adding that reporting from security firms indicates that the health care industry is not prepared technically to combat criminals' basic cyber attacks as well as being unprepared for sophisticated cyber attacks from so-called advanced persistent threats, like nation states or well-funded organized cyber crime groups.

'The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely," the Bureau stated.

Among the targets of the cyber criminals are patient medical records, billing and payment organizations, and intellectual property.

Additionally, security analysis has revealed that multiple elements of health care industry equipment and products have been compromised in cyber attacks, including radiology imaging software, digital video systems, faxes, printers, and security application systems, like virtual private networks, firewalls and routers.

"Once medical devices are compromised, malicious traffic is transmitted through VPNs and firewalls," the FBI said. "The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise."

According to the Ponemon Institute, a data security firm, some 63 percent of the health care organizations reported a data breach in the past two years and an average loss estimated to have cost about $2.4 million per data breach. Most of the cyber attacks produced theft of information assets and 45 percent that nearly half of the organizations surveyed failed to put security measures in place to protect patient records.

Another survey found that over 2 million health care records were compromised.

"Cyber criminals are selling the information on the black market at a rate of $50 for each partial [electronic health record], compared to $1 for a stolen social security number or credit card number," the FBI said adding that electronic health records are used in filing fraudulent insurance claims, obtaining prescription medication, and for conducting identity theft activities.

Detecting the theft of electronic health records also is difficult to detect and takes nearly twice as long as uncovering identity theft.

The FBI cyber notice urged companies to report cyber attacks or other suspicious criminal activities to Cyber Watch or Cyber Task Forces in their regions.

The Department of Health and Human Services, meanwhile, recently conducted a cyber attack exercise involving several health care providers and related companies.

The exercise, called CyberRX, revealed that many companies and agencies have difficulty getting cyber threat information and then are hampered by communications problems in dealing with the affects of cyber attacks on health care networks.

The exercise attack scenarios included simulations of cyber intrusions to medical devices, health

HIPAA SECURITY BRIEF

By Computer Networks, Inc. May 20, 2015 Volume 1, Issue 5
Serving Hampton Roads since 2004

information systems, health exchanges and Healthcare.gov website.

Participants included HSS, Athena health, Children's Medical Center of Dallas, Cooper Health, CVS Caremark, Express Scripts, Health Care Services Corp, Highmark, Humana, United Health Group, and WellPoint.

Jim Koenig, a cyber security expert with Booz, Allen Hamilton who took part in the exercise, said the exercise also revealed that the U.S. national cybersecurity framework for critical infrastructure is not sufficient to support healthcare organizations against current cyber threat.

"The growing adoption of new and connected health information technologies and widespread use of mobile devices continue to increase the industry's exposure to potential attacks," Koenig said.
— Bill Gertz
April 22, 2014
www.FlashCRITIC.com

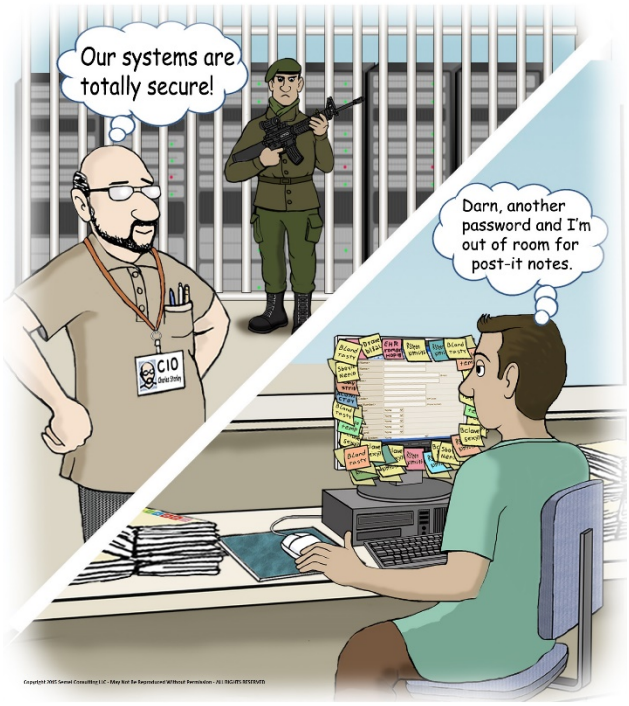
Security By Walking Around

by Mike Semel

When we think Cyber-Security we logically think about technology tools to block North Korean or Chinese hackers from breaking into our networks. Those breaches make the news because they are so unique. What is much more common are users doing stupid things that neutralize your investment in security tools.

Every business has data that is regulated, sensitive, or confidential. It doesn't matter why you want to protect it, although in regulated industries like health care you must follow specific rules. More than half of the HIPAA Security Rule protecting electronic data are Administrative safeguards – policies, procedures, and training— with the rest shared between Technical and Physical safeguards. Surprised?

An effective way to find out what your users are doing is to walk in their shoes, or, more accurately, sit in their seats. Take a walking tour of your office, go into cubicles and offices, and sit at the desks. Get management support, because executives are sometimes the worst culprits. Look around. Are there passwords on post-it notes on the monitor? Under the mouse pad or keyboard? Written on the calendar next to the desk?



Tell an employee you need to check their password to see if it meets the company requirements. Will they give it up?

Jiggle their mouse. Can you get right into Windows without entering a password?

What kind of physical security do you have? Are servers behind locked doors? Are visitors required to show ID? Are they escorted after they are admitted to your office? I have walked through many 'secure' facilities, wearing a suit and looking at my cell phone, never being challenged by many

people who saw me but were too afraid to ask who I was and why I was alone.

These all seem too simple to be problems, but every question ties back to a client engagement we have had where Chief Information Officers, IT Directors, Office Managers, doctors, and business owners have been shocked.

They have all said that *THEIR* users would never do things like *THAT*. Then we take the walk and show them security lapses are taking place throughout their office. Many complain about how much money they have spent on Security only to have their users come up with ways to make the investments worthless.

The simple solution is to just TAKE A WALK and address any security violations you see.

Policies

You don't need complex policies unless you have to comply with regulations such as HIPAA or financial industry requirements. Simple policies that users are not allowed to have passwords visible, must have automatic lockout enabled, and must log off when they walk away from their computer should be communicated, audited, and enforced. Employees must challenge visitors. They must not plug in a thumb drive they found into your computer. Check users periodically to let them know you are serious.

Training

Whenever you hire someone, make sure they get cyber-security training. At least twice each year, get your staff together and talk about cyber security topics they are likely to encounter, like someone asking for their password, receiving a phishing e-mail, finding a thumb drive, or seeing an unfamiliar visitor wandering through the office.

Reminders

Keep everyone's 'cyber-radar' at a high level. Talk about security in your staff meetings. Put up signs or use video screens to remind everyone to be vigilant.

And, every month or two, take the walk.

Former Hospital CFO Ordered to Pay $4.5M for Meaningful Use Fraud

Former Shelby Regional Medical Center CFO, Joe White has been ordered to pay more than $4.5 million in restitution for his role in a meaningful use fraud scheme, TV Station *KXXV* first reports. White pleaded guilty for directed its EHR vendor, eCareSoft and hospital employees to manually enter data from paper records into the EHR system after the patient was discharged to meet the MU thresholds criteria. Additionally, White also made false statements regarding other hospitals had successfully converting to EHR.

The false attestation resulted in CMS paying Shelby Regional $785,655 in January 2013. Medicaid and Medicare EHR incentive programs paid hospitals operated Dr. Mahmood, including Shelby Regional $16,794,462.66 for fiscal years 2011 and 2012.

In November, Mr. White also pleaded guilty to aggravated identity theft for using an employee's name to falsify documentation for the incentive funds that Shelby Regional received, according to the report. Shelby Regional Medical Center's owner, Tariq Mahmood, MD was sentenced in March to more than 11 years in prison for healthcare fraud, conspiracy to commit healthcare fraud and identity theft. Dr. Mahmood received nearly $313,000 in Medicare reimbursements from false claims.

www.kxxv.com

HIPAA SECURITY BRIEF

By Computer Networks, Inc. May 20, 2015 Volume 1, Issue 5
Serving Hampton Roads since 2004

The total budget request (PDF) for the Department of Health & Human Services (HHS) is $83 billion. This includes $43 million for the Office for Civil Rights (OCR) which is a $4 million increase over the 2015 budget. The increase will help support the permanent HIPAA audit process. OCR conducted a pilot program to ensure that its audit functions could be performed in the most efficient and effective way, and in FY 2015 will continue designing, testing, and implementing its audit function to measure compliance with privacy, security, and breach notification requirements," according to the authors of the budget brief report. "Audits are a proactive approach to evaluating and ensuring HIPAA privacy and security compliance." OCR continues to use HIPAA fines to expand the audit process OCR has authority to enter into resolution agreements that include payment of a resolution amount and corrective action plans, as well as imposing civil monetary penalties for violations of the HIPAA Rules. OCR collected $8 million in settlements in FY 2014 – an amount based on several unusually large agreements – and anticipates collecting $5.5 million in settlements in FY 2015. OCR retains and expands these collections to support overall HIPAA enforcement activities," For those who wrote off the HIPAA audits due to delays, this should be a wake-up call. The audits are going to happen and if the budget is approved, should increase in scope in 2016. Now is the time to prepare your organization.

Security Risk Analysis

A Security Risk Analysis (SRA) is a requirement for HIPAA compliance and for Meaningful Use compliance. Furthermore, you are required to update the SRA regularly and to have remediated the problems you found during your SRA.

If this sounds foreign to you, or if you know you are not in compliance, NOW is the time to fix the problem. Do not wait until CMS or OCR (the Office for Civil Rights) are standing in your office asking for your Polices and Procedures and evidence of compliance and remediation.

We have partnered with Semel Consulting to perform HIPAA Security Risk Assessments. Call us at 757-333-3299 x200 for more info.

HIPAA, coupled with easy Internet access, has changed the way you MUST look at your Information Technology and the security of your medical Practice.

It only takes moments for a Data Breach to happen. Can your Practice survive the consequences, such as huge fines and negative publicity, which comes with disclosing that you have lost Patient data?