Robinson+Cole

Data Privacy + Security

July 9, 2015

Data Privacy + Security Insider

HEALTH INFORMATION

Survey: Majority of healthcare organizations experienced a significant security incident in recent past

The Healthcare Information and Management Systems Society (HIMSS) recently released the results of its 2015 HIMSS Cybersecurity Survey. The survey results are based on the response of 297 professionals, each of whom plays a role in information security in a large healthcare organization. Key findings from the HIMSS survey include the following:

- Approximately two-thirds of respondents stated that their organization has experienced a significant security incident. The majority of these incidents were detected within 24 hours. Approximately 62% of security incidents involved a limited disruption to operations and approximately 20% of security incidents resulted in a loss of patient, operational or financial data.
- Negligent insiders comprised the largest source of a security incident, but 64% of respondents also experienced a security incident involving an external actor. Social engineering, online scams and hacking were reported as some of the external actors involved in a security incident.
- 87% of respondents indicated that information security has increased as a business priority. However, a majority of respondents reported that lack of personnel is a barrier to information security. A majority of respondents also reported that lack of financial resources is a barrier to information security.
- Respondents used an average of 11 technologies for information security. These include firewalls, anti-virus software, and encryption of data in transit and at rest.
- Approximately half of the respondents reported that a security incident was addressed solely through an internal investigation, however more than half of survey respondents reported involving third party vendors or law enforcement in connection with a security incident.
- A majority of respondents reported that their organization has a full-time information security professional.

- Almost 60% of respondents received threat intelligence through word-of-mouth.

HIMSS is a non-profit organization with a focus on better health through information technology.

– Pamela H. Del Negro

Connecticut legislation establishes statewide Health Information Exchange

Effective October 1, 2015, this legislation contains several provisions to encourage the free exchange of patient health information among providers and consumers. Hospitals, health systems, and electronic health record (EHR) providers are prohibited from "health information blocking," and this legislation establishes that such action is an unfair trade practice. Health information blocking is defined as either knowingly (1) interfering or engaging in conduct reasonably likely to interfere with a patient's, health care provider's, or other authorized person's ability to access or use an EHR or (2) using an EHR to both steer patients to affiliated providers and prevent or unreasonably interfere with patient referrals to unaffiliated health care providers. This legislation excludes from the definition of health information blocking referrals between providers participating in an accountable care organization or other value-based care model.

P.A. 15-146 also establishes a statewide health information exchange operated by the Department of Social Services. The establishment of the exchange is subject to the authorization of bond funds by the Connecticut General Assembly and approval by Connecticut's Bond Commission. The goals of the exchange include securely allowing real-time access to patient health information across all provider settings, enabling patients to access their health information at no cost, providing real-time alerts and other tools in support of care coordination efforts, reducing costs associated with preventable readmissions, and promoting EHR interoperability. Within one year of the exchange's launch, hospitals and clinical laboratories must have an EHR capable of connecting to the exchange and must begin the process of participating in the exchange. Other health care providers with EHR systems able to connect to the exchange must begin the process of participation within two years of the exchange's launch.

This legislation also requires each hospital that has an EHR system capable of exchanging electronically patient health information to take all reasonable steps to enable the bidirectional and secure exchange of a patient's electronic health information to all other health care providers furnishing services to the patient that maintain EHR systems capable of exchanging such records. Such information exchange must include laboratory and diagnostic tests, radiological and other imaging results, continuity of care documents, and discharge documents. While this legislation requires each hospital to implement technology already purchased to accomplish this exchange of information, it does not require hospitals to purchase additional software or equipment. Under this legislation, a hospital's failure to take reasonable steps to comply with these requirements will be deemed evidence of health information blocking.

– R+C's Health Law Group

Connecticut legislation requires consumer health information website

Effective October 1, 2015, this legislation requires the Connecticut Health Insurance Exchange (HIX) to establish, by July 1, 2016, a consumer health information website that contains information comparing the quality, price, and cost of health care services among health care providers in Connecticut. The HIX website must include price and cost information for the most common inpatient diagnoses and procedures, outpatient procedures, and surgical and imaging procedures based on a list published by the Department of Public Health (DPH) and the Insurance Department (DPH List). This information will be listed by health care provider and categorized by third-party payer. The HIX website must also include information to assist consumers in making informed health care decisions, such as what to consider

when choosing a health care provider, as well as links to the Joint Commission and Medicare websites, where consumers can obtain information to compare the quality of health care providers. The information must be publicized in a language and format understandable to the average consumer. Notwithstanding the above, the legislation allows the HIX sole discretion on the manner and timeframe for posting information to the consumer health website.

Under this new legislation, as of January 1, 2017, hospitals will be required to inform a patient of the right to request cost and quality information at the time of scheduling a diagnosis or procedure for nonemergency care that is on the DPH List. If the patient requests such information regarding the diagnosis or procedure, a hospital must, within three business days, provide the patient information on (1) the amount the patient will be charged if uninsured, including the amount of a facility fee; (2) the Medicare reimbursement amount; (3) if the patient is insured, the allowed amount and the insurer's contact information so that the patient may obtain additional information regarding charges and out-of-pocket costs; (4) the hospital's Joint Commission composite accountability rating and Medicare star rating; and (5) the website addresses for the Joint Commission and Medicare hospital compare tool. If the patient is insured and the hospital is out-of-network under the insurance policy, the hospital's notice must also state that out-of-network rates may apply.

– R+C's Health Law Group

DATA SECURITY

FTC announces data security guidance for businesses

We (and others) often comment on the Federal Trade Commission's (FTC) increased enforcement activity of data security issues, particularly with the Wyndham and LabMD cases, and the fact that it is enforcing data security without specific regulations. The FTC previously issued guidance in *Protecting Personal Information: A Guide for Business* and just issued its *Start with Security: A Guide for Business*on data security.

In the guide, the FTC points out that more than 50 law enforcement actions have been settled by the FTC and that the settlements are lessons for businesses to learn from when it comes to data practices. The 10 lessons the FTC specifically list are:

1. Start with security.
2. Control access to data sensibly.
3. Require secure passwords and authentication.
4. Store sensitive personal information securely and protect it during transmission.
5. Segment your network and monitor who's trying to get in and out.
6. Secure remote access to your network.
7. Apply sound security practices when developing new products.
8. Make sure your service providers implement reasonable security measures.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise.

10. Secure paper, physical media, and devices.

Although the guide is rather basic when it comes to data security, all businesses should review the guidance and compare it to existing security practices. It is also a great document for the C-Suite and board that may not be conversant in IT lingo to review for a basic understanding of the risks associated with data and to pose questions about the company's data security practices.

One thing is certain: if the FTC issues the guidance, it is a no brainer to follow it and exceed it as it is a roadmap of the FTC's data requests in an enforcement action.

– Linn Foster Freedman

Password best practices – I know, AGAIN!

With the uptick in high profile security breaches like the Office of Personnel Management, Target, JPMorgan and others, it is easy to become desensitized to the constant risk our cyber lives pose both personally and professionally. Information Technology departments have been rallying the battle cry about the necessity of using strong, complex passwords for decades now, to the point where discussing password best practices has become cliché. However, weak password practices continue to be one of the largest threats to both individual's and business' cybersecurity.

According to Verizon's 2015 Data Breach Investigation Report, credential hacking is still the most common threat action. When you consider the number of devices, websites and systems you have a password to it is not hard to appreciate the need for good password practices. Outlined below are the Dos and Don'ts to creating and maintaining strong, complex passwords, all commonly considered best practices by security experts.

Do:

- Create passwords that are a minimum of 10 characters long, preferably longer
- Use mixed case, alpha numeric AND special characters (#, !, @)
- Create a unique password for every device, website and/or system that requires authentication
- Choose multi-factor authentication whenever possible
- Change your passwords often, preferably every 60-90 days
- Use a password checker like Microsoft's

Don't:

- Use dictionary words or sequential numbers (i.e. password or 123456)
- Use proper names in your password
- Choose to allow a website, system or web browser to 'remember you, save your password, etc.'
- Reuse your passwords

- Write your passwords down anywhere

Example:

To create complex, unique, strong passwords that are easy to remember use a pass phrase and inject an identifier that is website or system specific.

mutatis mutandis becomes mU+@+15mU+@nd15

This is certainly a complex password. Now add the unique identifier. If this password was to be used for an email account you might use mU+@+15emailmU+@nd15. If for a shopping website you might use mU+@+15sitenamemU+@nd15 and so on.

– Sean C. Lawless

DATA BREACH

OPM data breach update: OPM shuts down background check system

The OPM announced this week that it is temporarily shutting down its background security clearance system, e-QIP, as vulnerabilities were found during a review of systems. Presently, according to OPM, the vulnerabilities did not lead to any type of exploitation of the system.

The shutdown will delay background security checks for those individuals who have applied for government security clearances.

– Linn Foster Freedman

CYBERSECURITY

The FBI has been busy

Here are several stories for the good guys~

The FBI and U.S. Attorney's Office for the Southern District of New York announced yesterday (July 8, 2015) that VLADIMIR TSASTSIN pled guilty to wire fraud and computer intrusion charges "arising from his operation of a massive and sophisticated Internet fraud scheme that infected with malware more than four million computers located in over 100 countries." The malware altered the settings on the infected computers which allowed TSASTSIN and other defendants the ability to hijack users' Internet searches, reroute the searches and receive payment for the rerouted Internet traffic. TSASTSIN will be sentenced in October.

The FBI and the U.S. Attorney's Office for the Southern District of New York have also announced that ALEX YUCEL, the owner of "Blackshades" which sold and distributed malware known as "RAT" to cybercriminals worldwide for $40 a piece, was sentenced in Manhattan federal court on June 23, 2015 to 57 months in prison, as well as three years' suspended release and forfeiture of $200,000 and computer equipment used to commit the crimes. The RAT malware could be installed on a user's computer to infect the computer and then spread the malware to other computers—just like a rat.

YUCEL was arrested in Moldova in November 2013 for computer hacking and plead guilty in February, 2015. According to the FBI press release, Yucel was the first defendant ever to be extradited from Moldova to the U.S.

– Linn Foster Freedman

FBI warns of continued use of Cryptowall ransomware schemes

The FBI's Internet Crime Complaint Center recently issued an alert "Criminals Continue to Defraud and Extort Funds from Victims Using Cryptowall Ransomware Schemes" that indicates that the Center continues to receive complaints about the spread and infection of the ransomware known as Crypotwall. The Center warns that Cryptowall is "the most current and significant ransomware threat targeting U.S. individuals and businesses." The ransomware has been active since April, 2014. Between April of 2014 and June of 2015, the Center received 992 complaints about Cryptowall, with reported losses of over $18 million.

The way Cryptowall works is that an individual (usually an employee) clicks on an infected advertisement, email or attachment, or visits an infected website. The ransomware is introduced and infects the employee's computer and encrypts the individual's files or network system. The individual is then sent a message that with the payment of $200-$10,000, the encryption key will be given to release the data. The ransom is usually paid in virtual currency, such as Bitcoin. Many companies have paid the ransom as it is less expensive than retrieving data with other means, such as back-ups. It is important to contact the FBI if you have been a victim of any type of ransomware, including Cryptowall. Most importantly, one of the best measures (besides best security practices) to protect your business from any type of malware or ransomware is to train your employees not to click on any suspicious emails, attachments or websites.

– Linn Foster Freedman

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

---