Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

March 24, 2016

CYBERSECURITY

Third Health Care Entity Becomes the Victim of Ransomware

The list of health care entities that have become (and will become) victims of ransomware is rapidly growing. The predictions from experts are that the list will grow exponentially into the future.

Last week, Methodist Hospital, located in Henderson, Kentucky, announced that it has become the third health care entity in recent weeks to be victimized by ransomware. The first was Hollywood Presbyterian Medical Center in Los Angeles, California (view related posts here and here), which paid $17,000 to the hackers to regain access to its electronic medical system, and the second known victim was Ottawa Hospital, which reported that it wiped the drives of the affected computers in order to regain access to its data.

Methodist Hospital declared an internal state of emergency and has announced that the FBI is investigating the case. It has been reported that the ransomware involved was able to lock patient files, and the hackers demanded money to unlock them. A spokesman from Methodist Hospital has confirmed that the hackers copied the patient records first before locking them. It is reported that the hospital has not decided yet whether to pay the ransom or not.

Despite declaring an internal state of emergency, the hospital was able to activate its backup system and states that it is operating as usual.

We anticipate that ransomware will continue to be a growing problem for health care entities in the future. The valuable lesson learned here is the importance of having a solid backup system and testing it frequently.

— Linn Foster Freedman

FBI and Traffic Safety Administration Issue Warning about Car Hackings

On March 21, 2016, the FBI and the U.S. National Highway Traffic Safety Administration issued a public safety announcement outlining the dangers of cars getting hacked.

The announcement follows media reports about two security researchers being able to hack into vehicles and remotely control them. It explains that, because new vehicles have more sophisticated technology, “it is important that consumers and manufacturers maintain awareness of potential cybersecurity threats.”

Issues explained in the announcement include how computers are used in vehicles, how attackers can access vehicle networks and driver data (Bluetooth, Wi-Fi, or mobile device), recently demonstrated remote exploits (engine shut down, disable brakes, steering, door locks, turn signal, radio, GPS, and HVAC), the response of the manufacturer, cybersecurity recalls and consumer action, how consumers can minimize vehicle cybersecurity risks, and consumer awareness, including contact information if you suspect your car has been hacked.

All in all, very informative for anyone who owns and/or drives a car.

— Linn Foster Freedman

FBI Issues Warning to Law Firms

The FBI has issued a private industry notification to law firms indicating that a cybercrime insider trading ring is targeting "international law firm information used to facilitate business ventures." According to the FBI, "[T]he scheme involves a hacker compromising the law firm's computer networks and monitoring them for material, non-public information…This information, gained prior to a public announcement, is then used by a criminal with international stock market expertise to strategically place bids and generate a monetary profit."

The FBI related that "In a recent cyber criminal forum post, a criminal actor posted an advertisement to hire a technically proficient hacker for the purposes of gaining sustained access to the networks of multiple international law firms."

FBI warnings are a heads up to the private industry about specific risks. Law firms may wish to heed this one.

— Linn Foster Freedman

HIPAA

Feinstein Institute Hit with $3.9M Fine from OCR for HIPAA Violations

Following the investigation of a self-reported data breach involving the loss of an unencrypted laptop containing the protected health information (PHI) of 13,000 individuals, the OCR slammed the New York-based biomedical research Feinstein Institute with a whopping $3.9 million fine. The Feinstein Institute also agreed to a Corrective Action Plan that addresses compliance with the HIPAA Security Rule, including completion of a security risk assessment and implementation of a risk management program with policies and procedures to address data security.

The laptop in question was password protected but not encrypted and, therefore, did not fall within the safe harbor for breach notification. The laptop contained the names, Social Security numbers, and medical information of patients and participants in research projects. It was stolen out of an employee's car. The OCR noted that the security measures and policies and procedures of The Feinstein Institute did not address removable media, such as laptops.

This case is another example of the importance of security measures related to removable media and implementation of encryption technology as a potential risk management tool.

— Linn Foster Freedman

OCR Announces New Round of HIPAA Audits—Get Ready Now

The Office for Civil Rights (OCR) has been stating publicly for some time that it will gear up for its second round of HIPAA audits, and the time has come. The OCR has officially started the next round of audits of covered entities. Round two will include audits of business associates for the first time.

Although business associates have been regulated entities under HIPAA since 2013, there have been no enforcement fines and/or penalties assessed against a business associate by the OCR to date.

The OCR has given covered entities and business associates time for compliance, and this new round of audits will not be as kind as the last. We have seen a change in the tone of investigations and enforcement actions by the OCR in the last two years, and it is losing patience with covered entities and business associates being lax with compliance.

Although the new audits will include the old reliable questions, we anticipate that the OCR will look deeper into covered entities' and business associates' compliance with the Security Rule, including completing a security risk assessment, ongoing risk management, frequent training of employees, and business associate agreements. All of these areas have been a focus of the OCR in the recent past, and such is evident from the most recent fines and penalties assessed against covered entities.

Being part of an OCR audit or investigation is time consuming, disruptive, and uncomfortable, even for the most compliant. Get your ducks in a row now and be ready. Both covered entities and business associates would do well to review their HIPAA compliance programs, with a focus on risk assessments, risk management, employee training, and business associate agreements.

— Linn Foster Freedman

DRONES

FAA Authorizes Mountain Aviation to Conduct Commercial Drone Operations

The Federal Aviation Administration (FAA) has certified the first airline to conduct commercial drone operations. Mountain Aviation has been flying private jets for over 23 years, and now, it will offer commercial drone services for aerial mapping, agricultural support, industrial inspections, aerial video, search and rescue, energy system inspections, and forestry and wildlife monitoring. Gregg Fahrenbruch, CEO of Mountain Airlines, said, "After two decades as a global leader in private jet charter we are excited to bring our technology based aviation safety systems to the long unregulated and emerging commercial [drone] market." Mountain Aviation is one of the few aviation companies that holds the ARGUS Platinum Safety rating. We are sure to see more commercial drone operations popping up all across the country.

— Kathryn M. Rattigan

Sports Industry, Untapped Area for Drone Use, Sure to Expand

Many industries are starting to explore a new area for drone operations, including the sports industry. Slowly, but surely, the use of drones for live sports coverage is expanding. In 2014, drones were used to film skiing and snowboarding events at the Winter Olympics, as well as at the Formula One Races, the X Games, and the AMA Supercross. The NFL currently uses CableCam systems (i.e., a computer-controlled and cable-suspended camera system hovering above the field), but these CableCam systems take a very long time to set up, are very expensive, and have limited scopes of vision due to the cable-suspended camera system.

So why doesn't the NFL (and other sports leagues) start using more drones for better coverage? Well, as currently written, the Federal Aviation Administration's (FAA) drone regulations make it quite difficult to operate drones in stadiums, arenas, and other sports venues. The biggest issue with drone operation in these areas is safety and privacy of the crowds surrounding these games and matches. However, commercial drone operators can apply for a FAA 333 Exemption certificate (i.e., an airworthiness certificate for certain drones to perform commercial operations prior to the finalization of the FAA small drone rule) to operate a drone for sports coverage purposes. But these FAA 333 Exemptions are few and far between due to the safety issues and room for operator errors. As drone use continues to expand, drone developers will continue to work on safety measures and privacy practices that will integrate drones into live sports broadcasts in a more efficient way. For now, we will keep watching the games and keep watching the skies.

— Kathryn M. Rattigan

New Drone Bill Proposed in Utah—Police Could Potentially Shoot Drones Out of the Sky

The latest drone bill popped up in Utah this month, and would allow police officers to shoot drones down out of the sky. This is an interesting proposal because there is currently litigation pending in Kentucky regarding a private citizen shooting down a drone that hovered above his "personal airspace." Senator Wayne Harper introduced this bill to establish criminal penalties for misusing drones and allowing first responders to "neutralize" the drone. The types of misuse contemplated by this bill include voyeurism, flying them within 500 feet of a correctional facility, photographing near crowds of more than 500 people, and flying them within three miles of a wildfire. Harper says in support of his bill, "We've had drones that have followed somebody down the street—watch them as they close the door and then watch them through the window of their house after they have gone inside." Commercial drones that obtain Federal Aviation Administration (FAA) licenses would be exempt from this bill. The concern with this type of regulation is that it could pose more of a safety threat than the threat originally posed by the drone. However, Harper's bill includes language forbidding police officers from disabling or destroying drones if they would injure people or animals. If this Utah bill passes, Utah would be the 27th state to pass drone safety and privacy laws, including states like California, Florida, and Arkansas.

— Kathryn M. Rattigan

ENFORCEMENT + LITIGATION

FTC Issues Warning to App Developers about Use of Microphone Software—It Monitors Consumers' TV Use without Their Knowledge

Most people don't think about the microphone on their mobile phone unless it isn't working. Most people don't know that, if it is on, it is working all of the time and is capturing private data that it has access to.

Last week, the Federal Trade Commission (FTC) issued warning letters to app developers using the software known as Silverpush. According to the FTC, Silverpush is software that "is designed to monitor

consumers' television use through the use of 'audio beacons' emitted by TVs, which consumers can't hear, but can be detected by the software."

According to the FTC, Silverpush is capable of tracking detailed information about the content of television usage if a user's mobile device is turned on while the user is watching TV. It can also produce a log of the consumer's television viewing habits so the usage can be analyzed for targeted advertising purposes. "These apps were capable of listening in the background and collecting information about consumers without notifying them," said the FTC.

The FTC warned the app developers that they should provide notice to users about the listening capabilities of the software and get user's permission before using the microphone function. If they don't, the FTC warned that they could be in violation of Section 5 of the FTC Act.

To avoid the listening feature of the microphone on your mobile phone, check that microphone setting or turn off your phone while you are watching TV or doing anything else that does not require the use of your microphone.

— Linn Foster Freedman

Cyber Prosecutions Update

The feds have been busy on the cyber prosecutions front. First, on March 18, 2016, the FBI announced that a multi-agency collaborative effort blew up an identity theft ring whose leader was an inmate in a Georgia prison. The ring defrauded the federal government up to $1 million. The ring had employees in big box stores with access to customer credit cards providing credit card information which was used to produce counterfeit identification documents so those committing the fraud could pose as real store members. Then the criminals were able to obtain new credit cards to purchase gift cards, gas, and groceries. Nineteen Atlanta residents were convicted of their part in the scheme and will be sentenced in the near future.

On March 21, 2016, Virginia federal prosecutors announced that three Syrians have been charged with hacking attacks in the United States, including a plot to impersonate an Associated Press tweet about an explosion at the White House which caused a dip in the stock market. The hackers are alleged to have hacked into multiple Twitter accounts of well-known media outlets.

Two of the hackers were accused of trying to hack into White House computers on multiple occasions. They are also alleged to have attempted to extort money from at least 14 hacking victims. Arrests have been issued for all three hackers, two of whom are believed to be located in Syria and the third in Germany.

The FBI has added two of the hackers to its Cyber's Most Wanted List and is offering a reward of up to $100,000 for information that leads any of their arrests.

Finally, an analyst that was previously employed with the Federal Reserve Bank of Chicago pled guilty last week to charges that he stole documents related to tracking the health of financial institutions. He printed numerous documents and took the documents home on his last day on the job at the Federal Reserve while he was negotiating employment with a new outfit. He is banned for 10 years from working at a banking institution insured by the FDIC.

— Linn Foster Freedman

SOCIAL MEDIA

Report Says Social Media One of Biggest Security Threats to Companies

A new report released by Osterman Research, sponsored by Actiance, GWAVA, and Smarsh, tells us that social media is one of the biggest security threats for companies. Malware is increasingly making its way into companies via their employees' social media accounts. Overall, the report found that only 54 percent of companies have a written social media policy governing its employees' use of social media in the workplace. That may not surprise you, but the report also found that 18 percent of companies have had malware placed on their network through social media, while 25 percent have had malware enter its network from an unknown origin. The report seems to suggest that the unknown origin is more likely than not a social media website.

What ways can malware enter your network through social media? Well, in ways like a Twitter link shortener (i.e., an online application that converts a regular URL (the web address that starts with http://) into its condensed format) or a fake social media account. Smarsh's vice president of marketing said, "It's clear that securing the perimeter of social media communications is a critical part of risk management. Organizations need to know how their employees are using social media for business communications to protect both the company and the employee."

This is not to say that social media is not also beneficial to a company. The report also states that social media leads to faster decision-making capabilities, better customer service, and improved corporate culture. The key to take away from this report is to be proactive in your employees' use of social media and be aware of the threats it may pose so you can get out in front of the malicious hackers.

— Kathryn M. Rattigan

INFORMATION GOVERNANCE

Developing Information Governance Efforts

In an information governance model, there are business-focused components and aspects, and there are technology-focused components and aspects. Information Governance isn't just technology driven, nor is it solely business driven. It is a partnership between business and technology. Both must be present in the program.

The Business Side

Diving into the business side, the first major aspect to Information Governance are the stakeholders. There are many, many stakeholders to Information Governance, but mainly they belong to five specific categories (Business, Legal/Compliance, Records & Information Management, Privacy/Security, and IT), which may or may not cover all stakeholders to Information Governance.

The second major aspect on the business side are the business-focused components that bolster an Information Governance program and are critical to its success. These include Change Management, Communication, Organizational Learning and Training, Standards and Best Practices, Help Desk, and/or Frequently Asked Questions, and are all bolstered by a solid and (generally) iterative project management methodology.

The last major aspect on the business side is a process to call out the things that need to be defined and established at an organizational level to ensure ongoing success of the Information Governance program.

This includes Metrics, Policies, Procedures, Rules, and Roles, all with an underlying accountability matrix.

The Technology Side

On the technology side, there are basically four components: (1) Information Access, which could also be thought of from the alternative risk-based perspective of Access Controls ensures that the right people have access to the right information at the right time; (2) the Information Lifecycle, which includes version controls available, retention policies, storage principles managed, legal holds, and eDiscovery processes available, and eventual disposal or archival. Throughout the lifecycle of information, there must be an application of search, as a function of access, and the application of information protections.

Continuing on with the technology side, (3) structures should be in place, including the Information Architecture, Taxonomy, and Metadata, which must be applied and available in the technology. In addition, Formats, Protocols, and the Technology Architecture should be in place.

Finally, (4) the applications and software used to apply information governance practices, will need to be considered, such as APIs, or Web Services, that connect together disparate systems because most organizations have multiple systems. infrastructure is used to connect those systems so Networks & Connectivity are appropriate for the organization's needs are also a consideration. Underlying the infrastructure must be a particular focus on security.

Whatever model you use, it is important for every organization to consider an Information Governance Program for the life of its data.

— James Merrifield

PRIVACY TIP #27

Complying with the New Rhode Island Data Security Law

As we mentioned before, Rhode Island amended its Identity Theft Protection Act on June 30, 2015, which will become effective on June 26, 2016. Now is the time to think about and put processes in place for compliance with the law by that date. This includes implementing data security measures for the personal information of Rhode Island residents.

The biggest changes to the law from its previous version include the following:

1. Individuals affected by a data breach must be notified within 45 days of the breach. In the general scheme of state laws, this notification time period is one of the shortest, and a close eye should be kept on this deadline.

2. Any entity or person that "stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program" to protect the information. This basically means any employer in the State of Rhode Island must implement a data security program, as all employers hold the personal information, including the Social Security numbers, of its employees. This is similar to a Written Information Security Program (WISP) in Massachusetts, and a Comprehensive Information Security Program required in Connecticut. If you already have a WISP in place to comply with the Massachusetts data security regulations, you may want to update the WISP to include the new provisions in Rhode Island and Connecticut so the policy complies with the requirements of all three states.

3. There are very specific statutory requirements of what has to be in the security program. It must be in writing and include specific security requirements, including, but not limited to, access controls, security measures to protect the information from unauthorized access, use and disclosure, and processes around data retention and destruction.

4. Health insurance information and medical information are now included in the definition of personal information.

5. Notification to individuals must include information about the individual's right to file or obtain a police report, how to request a security freeze and fees that may be applicable for security freezes, and contact information for credit reporting agencies, remediation service providers, and the attorney general.

6. The attorney aeneral of Rhode Island must be notified in the event of a data breach involving more than 500 individuals.

7. Penalties for violation are $100 per record for a reckless violation and $200 per record for a knowing and willful violation. The attorney general may bring an action against the business or person in violation of the statute.

We have been helping clients with compliance with the new Rhode Island requirements. You may wish to review your data security measures and implement a written information security program that complies with the new Rhode Island law so you will be in good shape when it becomes effective on June 26, 2016.

— Linn Foster Freedman

For more thoughtful and timely discussions of legal news and perspectives on 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.