Robinson+Cole

Data Privacy + Security

July 2, 2015

Data Privacy + Security Insider

DATA BREACH

Connecticut Governor signs new comprehensive and strict data security law with extensive compliance obligations for companies, including breach notification

Yesterday, (June 30, 2015), Connecticut Governor Dannel Malloy signed into law Substitute Senate Bill 949, "An Act Improving Data Security and Agency Effectiveness" which requires state government contractors to implement extensive data security measures when receiving personal and/or health information from a state agency, and health care centers or other entities licensed to do health insurance business in the state, pharmacy benefits managers, third-party administrators and utilization review companies to implement a comprehensive information security program (CISP), as well as amendments to Connecticut's data breach notification law. The law is considered one of the most stringent data security laws in the country.

The new law is quite extensive and requires specific compliance by government contractors, health insurers, health care centers, any entity licensed to do health insurance business in Connecticut, pharmacy benefits managers, third-party administrators, utilization review companies and "any person who conducts business" in the state of Connecticut and applies to all residents of the State of Connecticut, no matter where the information is held.

The requirements and deadlines for compliance with the law are outlined here.

-Linn Foster Freedman

Rhode Island Governor signs new comprehensive Identity Theft Protection Act

On June 26, 2015, Rhode Island Governor Gina Raimondo signed Senate Bill S0134, the Rhode Island Identity Theft Protection Act of 2015, which substantially revises the old law, including breach notification.

Specifically, the new law requires municipal agencies, state agencies and any “person” that “stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident” to implement “a risk-based information security program” which “contains reasonable security procedures and practices…in order to protect the personal information from unauthorized access, use, modification, destruction or disclosure…”

The law further requires agencies and businesses to implement a written document retention policy and not retain personal information longer than is necessary for the purpose for which it was collected and destroying the information in a secure manner including shredding, pulverization, incineration or erasure.

In addition, all agencies and businesses that disclose personal information of Rhode Island residents to a third party must have a written contract in place with the third party ensuring that the third party has implemented and maintains reasonable security procedures and practices to protect the information.

If an agency or business suffers a data breach, the agency or business must notify individuals of the breach within **forty-five (45)** days of confirmation of the breach. This is one of the shortest periods of time in national data breach laws. Further, if the breach affects more than 500 individuals, the agency or business must notify the Attorney General, which is also a new provision.

Following Massachusetts, the law sets forth the specific requirements of the notification letter, including that the individual is entitled to file a police report and how to obtain a credit freeze.

Penalties for violation of the Act include a civil suit by the Attorney General and $100 per record for reckless violation of the Act and $200 for knowing or willful violation.

The Act becomes effective on June 26, 2016.

-Linn Foster Freedman

OPM sued by workers' union in proposed class action

The Office of Personnel Management (OPM) was sued this week in the D.C. federal court by its workers' union the American Federation of Government Employees (AFGE). Significantly, the suit named OPM Director Katherine Archuleta and Chief Information Officer Donna Seymour individually as negligently causing and contributing to the largest breach in government history. Naming the CIO directly in the suit certainly raises the stakes for IT professionals.

According to the suit, the AFGE claims that OPM has failed to reveal the full scope of the breach, including who was impacted and details about the information that was actually compromised.

The OPM continues to stick to its story that the breach affected approximately 4 million individuals' information, but other reports have estimated that all in, the breach affected up to 18 million individuals. It will be interesting to see if the suit is able to obtain clarity about the details.

-Linn Foster Freedman

Trump Hotels investigating credit card breach

Trump Hotel Collection, the luxury hotel brand owned and operated by Republican candidate for President Donald Trump, announced this week that it is investigating a credit card breach affecting its properties. It has been reported that the breach involved Trump properties in Chicago, Honolulu, Las Vegas, Los Angeles, Miami and New York and has been going on since February.

Although credit card companies are moving toward chip and pin technology to defeat the ongoing slaughter from hackers in stealing credit cards, until cards with the new technology flood the market, credit card theft and fraud will likely continue at an alarming rate while hackers try to make as much hay as possible with old cards.

-Linn Foster Freedman

DATA SECURITY

Audit reveals U.S. Treasury Dept. security infrastructure is weak

An annual audit conducted by the U.S. Government Accountability Office of the Fiscal Service Bureau, identified (9) nine new information security weaknesses in the U.S. Treasury Department's information systems that are used to manage sensitive data in connection with federal debt.

It was further reported that although these weaknesses aren't considered to be significant, the Department must address these information security weaknesses immediately, in order to protect sensitive data from being further compromised or accessed by future hackers.

After all, the Fiscal Service Bureau manages $18.2 billion of the national debt with a number of interconnected financial systems. The electronic data stored in these systems are used to process and track borrowed money and issued securities.

The audit found that the identified risks in connection with these system weaknesses primarily stemmed from individuals who have access to the Fiscal Service internal systems. The audit further revealed that some of these weaknesses may be related to a new ledger system, which was implemented in 2014.

It is important to note that earlier this month, the Office of Personnel Management (OPM) reported that hackers had accessed the personal information of more than 4 million federal employees. It's known now that the hackers also were able to access security clearance data. Apparently, the OPM has had a history of information security related weaknesses and is still working to address these and other vulnerabilities.

It's clear that the federal government has its work cut out in relation to securing its technology infrastructure. At present, 11 out of the OPM's 47 information technology systems are operating without a valid security authorization. This includes two systems responsible for processing background checks and security clearances.

The logical place to start is to find out who in the Fiscal Service Bureau and OPM currently have access to these internal systems, then re-evaluate if all these individuals should have permission to access these systems. The results of this exercise will no doubt be very surprising and eye-opening, but it must be done.

This is a warning example for all of us--whether we work in the federal government or not. After all, every organization deals with sensitive data and can be vulnerable to a security breach at any time. Of course, all organizations would be well served to conduct a security assessment of its current IT infrastructure.

If your organization needs assistance in planning such an assessment, please contact any of the team members here at R+C.

-Jim Merrifield

Effective information security governance: executive support a must

According to a very recent report by the Identity Theft Resource Center, the first half of 2015 alone saw 400 publicized security breaches with over 117 million records exposed. While most organization have ongoing initiatives to keep their names off the list, many are misguided in their approach – making the

effort almost entirely an IT project.

Numerous studies show a direct correlation between the maturity of an organization's security profile and the level of engagement and understanding by its board and/or executive management. The IT Governance Institute in its Board Briefing on IT Governance, 2nd Edition, states: "Security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."

In comparing the critical differences with respect to the effectiveness of a company's information security governance program, published author, Shon Harris, highlights the following distinctions common to successful organizations:

1. Board members understand that information security is critical to the company and requires regular updates on performance and security incidents

2. The officers and business unit managers participate in a risk management committee that meets regularly on the topic of information security

3. Executive management sets acceptable risk levels which are the basis for the company's security policies and related practices

4. Executive management holds business unit managers responsible for carrying out risk management activities for their specific business units

5. Critical business processes are documented along with the risks that are inherent in the different steps within the business processes

6. Employees are held accountable for any security breaches they participate in, either maliciously or accidentally

7. Security products, managed services and consultants are purchased and deployed in an informed manner and are regularly reviewed

8. The organization regularly reviews its business and security processes with the goal of continuous improvement

Engaging the C-Suite and board in the complexities and efforts of the entire organization, including IT is critical to managing an effective risk management program.

-Monte Monteleone

INTERNATIONAL PRIVACY LAWS

What European Union privacy reform means for U.S. Companies

The European Union (EU) General Data Protection Regulation (GDPR) is one step closer to replacing the EU's 1995 data privacy directive, known as 95/46/EU. In late June, the Council of Ministers from the EU member states approved a general approach to the GDPR. The European Parliament, the European Council and the European Commission (EC) are now negotiating the GDPR approach and wording, which is widely expected to result in enactment of a final regulation by early 2016, with an effective date a year or more later.

Once adopted, the GDPR regulation would apply directly to EU member states without the need for each state to pass legislation. This means one uniform set of EU data protection requirements for regulators,

businesses and individuals. This is different than the existing EU scheme under the 1995 data privacy directive, where each member state has slightly different requirements. That is because under EU law, a directive must be adopted by each state, and as a result, it is often modified, resulting in varying requirements. U.S. companies will benefit from the consistency the harmonized approach will bring, even if some of the requirements are stricter than the current EU directive.

U.S. companies are likely to focus on any further restrictions the GDRP makes in the U.S. safe harbor program allowing personal data to be transferred outside the European Union. Changes could include additional data protection and contractual provisions as well as binding corporate rules. It is expected that the U.S. Safe harbor scheme will survive, in substantially the same form, in part due to the large volume of U.S/U.K trade.

-Kathleen M. Porter

TELEHEALTH

Connecticut Enacts Act concerning the facilitation of telehealth

Public Act 15-88 is the first comprehensive law in Connecticut to address telemedicine (also referred to as "telehealth"), and to establish regulatory requirements for providing telehealth services, and mandates certain insurance coverage for such services. Telehealth is a mode of delivering health services to patients via information and communication technologies to facilitate the diagnosis, consultation and treatment, education, care management, and self-management of the patient's physical and mental health.

Under the new law, any of the following licensed professionals acting within their scope of practice and in accordance with applicable standards of care can provide services via telehealth: physicians, physical therapists, chiropractors, naturopaths, podiatrists, occupational therapists, optometrists, advanced practice registered nurses, physician assistants, psychologists, marital and family therapists, clinical or master social workers, alcohol and drug counselors, professional counselors, and certified dietician-nutritionists.

Requirements for Telehealth Services

Telehealth services must be conducted using real-time, interactive two-way communication technology and/or transmitting images and data recorded with a camera or other technology from the patient to the remote provider. The definition of telehealth expressly excludes the use of fax, audio-only telephone, text messaging, and e-mail. Telehealth providers must have access to or knowledge of the patient's medical history, as provided by the patient, and the patient's health record, including the name and address of the patient's primary care provider. Health care services rendered via telehealth must conform to the standard of care applicable to the provider's profession that would be expected for in-person care and, if the relevant standard requires the use of certain tests or a physical exam, such tests or exam may be carried out using appropriate peripheral devices. Providers are prohibited from prescribing schedule I, II, or III controlled substances via telehealth.

The new requirements include certain patient protections. During the first telehealth interaction, providers must inform their patients about the treatment methods and limitations of providing treatment via telehealth and obtain the patient's consent to using telehealth, to be documented in the patient's health record. At the time of each telehealth interaction, telehealth providers must request patient consent to disclose records relating to the telehealth session to the patient's primary care provider. If the patient does consent, such records shall be shared with the patient's primary care provider. The provision of telehealth services and maintenance and disclosure of related records must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended. Telehealth providers must provide patients with their license number and contact information. Facility fees may not be charged for telehealth services.

The legislation is clear that it should not be construed to prohibit (1) a provider from providing on-call coverage or consulting with another provider regarding a patient's care or (2) orders of health care providers for hospital outpatients or inpatients.

These requirements are effective as of October 1, 2015.

-Christopher J. Librandi + Meaghan Cooper

ENFORCEMENT + LITIGATION

The Computer Fraud and Abuse Act and the "Cannibal Cop": awaiting the Second Circuit's decision

The Computer Fraud and Abuse Act began as a federal criminal statute, but it has turned into an oft-used weapon in civil litigation. See U.S.C. § 1030, et seq. ("CFAA"). Now, criminal and civil litigants await the Second Circuit's decision on what exactly the CFAA covers.

Looking at statute's plain language, the CFAA applies when a defendant "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C).

How the statute applies to the real world is much more complicated. Does the CFAA apply when an employer gives an employee access to use computer files for work, but the employee uses those files to help a competitor? What happens when a police officer uses police databases for personal purposes even though department policy limits use for government investigations? Is such access "without authorization" and does it "exceed authorized access"?

The Second Circuit has not ruled on these issues in the civil or criminal context. In May, however, the Second Circuit heard oral argument in United States v. Valle, 14-4396-cr, a case in which the Court has the chance to answer these questions.

In Valle, a police officer, referred to as the "Cannibal Cop" because of his use of certain Internet chat rooms, was convicted of violating the CFAA when he used the police department's database to conduct his own personal searches. Did this violation of the department's data use policy violate the CFAA?

The Second Circuit has the opportunity in Valle to clarify the scope of the CFAA. We will update you on the CFAA and the Cannibal Cop when the Valle decision comes out.

-Nuala E. Droney

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.