Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

FBI Issues Flash Alert on Apache Struts Vulnerability

The Apache Struts vulnerability has been mentioned frequently in the media over the past month, as it is believed to have been involved in one of the largest and most damaging data breaches in history. The vulnerability, first disclosed in March 2017, is thought to have affected (and is still affecting) hundreds of corporate networks. The FBI has issued a flash alert requesting help from the private sector to track a group presently targeting older versions of the open source web application framework Apache Struts. *Read more*

Arkansas Surgery Center Hit with Ransomware

Arkansas Oral & Facial Surgery Center (AOFSC) was recently hit with ransomware that shut down access to its patients' health information and rendered some of its imaging files, including patient's X-rays, inaccessible. *Read more*

VIRTUAL CURRENCY

SEC Brings Fraud Action against ICO Creator

In its first lawsuit targeting Initial Coin Offerings (ICOs), the Securities and Exchange Commission (SEC) has filed fraud charges against the creator of the ICOs marketed as “REcoin” and “DRC.” The action, filed in the United States District Court for the Eastern District of New York on September 29, 2017, alleges that Maksim Zaslavskiy, operating through two wholly owned companies, raised over $300,000 from investors based on false claims the digital “tokens” or “coins” being marketed were backed by investments in either real estate or diamonds. According to the SEC’s complaint, not only were funds raised by the ICO not invested in any assets, the digital tokens did not actually exist. Despite representations by Zaslavskiy, no digital tokens had actually been developed or issued on a blockchain, leaving investors with no value in exchange for their payments. *Read*

October 12, 2017

FEATURED AUTHORS:

Linn Foster Freedman
Benjamin C. Jensen
Sean Lawless
Kathryn M. Rattigan
Matthew P. Rizzini

FEATURED TOPICS:

Cybersecurity
Data Security
Drones
Enforcement + Litigation
HIPAA
Privacy Tip
Virtual Currency

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

more

ENFORCEMENT + LITIGATION

Vermont AG Settles with SAManage for $264,000 for Delayed Breach Notification

The Vermont Attorney General's Office (AG) recently announced that it has settled with SAManage USA, a business support services company, for failing to timely notify 660 Vermont residents that their names and Social Security numbers were accessible through the online search engine Bing. *Read more*

DATA SECURITY

Is Blockchain the Answer to Identity Management?

Considering the recent Equifax data breach, which put an estimated 145.5 million Americans' identity at risk, mainstream media outlets are starting to ask an important question: if we can't stop data breaches, how do we protect our identity? According to data from the Identity Theft Resource Center, U.S. companies and government agencies have disclosed 1,022 breaches in 2017 so far. The idea that the Social Security number is the foundation of our identity is under more scrutiny than ever. Bloomberg reported recently that the Trump administration is considering ways in which it can replace the Social Security number as a means of federal identification. So, can blockchain technology solve our identity management (IDM) problem? Blockchain is the distributed public ledger-based technology that underlies applications such as the cyber currency Bitcoin. *Read more*

HIPAA

Business Associate Resold Fax Machine Containing PHI

Fax machines are still used in the medical community, and these days, faxing may be more secure than emailing, as hackers have not yet cracked the task of hacking into old fax machines. All kidding aside, fax machines have been, and continue to be, a risk to organizations because they have the ability to store data, just like copy machines.

An individual who bought a fax machine at a resale shop took it home and printed the fax transmission sheet off the fax machine. in doing so, the fax machine printed the health information of 20 patients of a physician who is part of a health system in Michigan. The documents

included their names, addresses, dates of birth, dependents, diagnoses, test results, and insurance information. *Read more*

DRONES

Congress Approves FAA extension to March 31, 2018

When we previously wrote about the Federal Aviation Administration Reauthorization Act, the deadline was set at the end of September. Just before the deadline, Congress approved a six-month extension of Federal Aviation Administration (FAA) taxes to give lawmakers more time to debate contentious, long-term airline policies. It is now set to expire on March 31, 2018, which will give legislators more time to assess items such as air traffic control management and pilot training.

FAA reauthorization bills were passed earlier this year by the House and Senate committees, which included UAS-related provisions. The authorization will be renewed for four more years, at least, if it is renewed. We will keep you updated on its status as it moves forward. *Read more*

Drone Industry Grows, the Fight for Control of the Sky Builds

It's now considered "cool" to fly a drone whether you are doing it for your business or as a hobbyist in your own backyard. When the Federal Aviation Administration (FAA) released the final rules for small unmanned aerial systems (UAS) operations back in August 2016, the price of a drone decreased and the number of drones on the market exploded. Now there are over 1.1 million consumer drones according to the FAA, and companies are using drones for everything from utility inspections to movie filming, agriculture, real estate, scientific research, and law enforcement. One big challenge for those in the commercial sector: uncertain regulations. *Read more*

PRIVACY TIP #109

Cybersecurity Tips for Small (and all) Businesses

I travel around helping businesses, both large and small, assess their cybersecurity risks and implement measures to protect data, reduce risk, and comply with applicable state and federal laws. In doing so, it is obvious that all businesses are struggling with managing data risks, and the time, resources, and tools necessary to combat the risks are daunting.

This is particularly true for small businesses, which don't have the same resources to devote to the problem. Nonetheless, there are

measures that small (and all) companies can take to reduce their risks.

Here is a general list of measures for a starting point. This is not an exhaustive list, but is a basic list to help you get started. Many companies feel overwhelmed with the prospect of starting a data privacy and security program. My attitude is that you have to start somewhere, take baby steps, and keep plugging along. The process is never "done," so make a commitment to start the process. Hopefully, this list will help you get motivated to do so:

- Map your high-risk data, such as Social Security numbers, drivers' licenses, financial information, health and insurance information—know where your high-risk data is in paper and electronic form so that as your highest priority you can protect your highest-risk data first.
- Conduct a security risk assessment to identify any vulnerabilities.
- Implement at least minimum security measures, including a fire wall, dual factor or two factor authentication, encryption, anti-virus and anti-malware software, password procedures (see previous blog about password tips here and here) and evaluate implementing a Bring Your Own Device Program, so a vulnerability patch system so patches are implemented in a timely manner.
- Put policies (that are legally required—limit what you call a "policy") and procedures in place (such as a written information security program) that comply with legal requirements or provide expectations and guidance for your employees on how you expect them to use your company assets .
- Make the policies and procedures understandable and available to employees.
- Educate your employees on data privacy and security, including phishing, and spear phishing and what their responsibilities are in helping the company protect its data. Encourage employees to be data stewards of the company.
- Make the employee education interesting and creative and bring your employees into the conversation so they feel engaged.
- Map the vendors that have access to high-risk data and enter into contracts with them that include security measures subcontractors and vendors are required to put in place to protect your data.
- Consider questioning high-risk vendors directly on security measures that they have in place to protect your data.
- Develop an incident response plan and team and a breach notification program.
- Consider obtaining cyber liability insurance.
- Put a data privacy and security team in place.

This list is a high-level starting point and is designed to be a basic checklist to assist small businesses to consider when starting a risk management program around data privacy and security. If you haven't started a program, hopefully this will help you get off the

ground.