Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

April 14, 2016

CYBERSECURITY

New Report Finds Executives "Placing Their Heads in the Sand" on Cybersecurity

A new report commissioned by Tanium and Nasdaq finds that 90 percent of corporate executives admit that they can't read a cybersecurity report and up to 40 percent of corporate executives do not feel personally responsible for cybersecurity for their organization. The report was the culmination of a survey of 1,530 nonexecutive directors and C-Suite executives in the U.S., U.K., Germany, Japan, and the Nordic countries. Following the issuance of the report, the chief security officer at Tanium said "they're really just placing their heads in the sand right now."

Further, the report concludes that executives do not feel that they are prepared to handle a major cyber-attack, and are primarily delegating data security to the organization's IT department.

Cyber intrusions and attacks are occurring with intense acceleration and sophistication. Governance of cybersecurity is a critical risk management strategy for every organization. The report shows that the C-Suite and board must get their heads out of the sand, educate themselves about cybersecurity, and take measures to protect the organization's data. The risk is not going to go away if you ignore it.

— Linn Foster Freedman

Vendor Management High on the Risk Management To-Do List

A new Ponemon study emphasizes the risk of third-party vendors that have access to company data. According to the survey "Data Risk in the Third-Party Ecosystem," companies are concerned about their third-party vendors, but more than one-third of the companies surveyed do not believe that the vendor will notify them if a data breach occurs.

The study showed that companies have difficulty with managing their third-party vendors, and even more challenges exist when trying to manage fourth-party vendors (and so on) that may have access to their data through the vendor, and might not even be on the company's radar.

Although it is common practice to include data privacy and security measures in third-party contracts to ensure vendors have appropriate security measures in place to protect company data, it is more difficult to evaluate how the vendor is protecting the data from unauthorized access, use, and disclosure by its vendor, and if it has appropriate contractual measures in place with the downstream vendors.

The Ponemon survey concludes that 73 percent of companies do not believe that a fourth-nth° vendor will notify them of an unauthorized access, use, or disclosure of company data.

Vendor management, including downstream vendors to the nth°, is essential to risk management and the protection of company data. Companies may wish to review the Ponemon study and consider making vendor management a high priority in their risk management program.

— Linn Foster Freedman

FBI Issues Another Warning of a "Dramatic Increase" in Phishing Spoofs of CEOs

We have consistently reported about increased phishing attacks through emails that purport to come from high-level executives, including CEOs. According to the FBI, the hackers use sophisticated social engineering to spoof company emails to "assume the identity of the CEO, a company attorney, or trusted vendor. They research employees who manage money and use language specific to the company they are targeting, then they request a wire fraud transfer using dollar amounts that lend legitimacy."

It is such a problem that the FBI has issued another warning about the scams, saying that there has been "a dramatic rise in the business email compromise scam or "B.E.C.," a scheme that targets businesses and has resulted in massive losses."

The FBI states that it has received complaints from victims in every state in the U.S. and at least 79 countries from 17,642 victims.

The losses associated with the email scams total more than $2.3 billion.

The most shocking statistic is that the FBI has seen a 270 percent increase in identified victims and exposed loss.

We too have seen a dramatic increase in phishing scams. Even the smallest of companies can be a victim. Employee awareness and education is key to combatting these schemes. Other tips from the FBI:

- Be wary of email-only wire transfer requests and requests involving urgency.
- Pick up the phone and verify legitimate business partners. (Yes, the phone on your desk still works!)
- Be cautious of mimicked email addresses.
- Practice multilevel authentication.

Hackers are getting more sophisticated and will continue to attack as long as they can make a profit. Employees can help protect their companies by increasing vigilance, using their gut instincts, keeping antennae up, and picking up the phone and not being afraid to ask the highest executives questions.

— Linn Foster Freedman

DATA BREACH

Experian Handling 70 Breaches a Week Resulting from IRS Phishing Scam

On March 1, 2016, the Internal Revenue Service alerted the business community of an email phishing scheme designed to convince employees to provide company-wide W-2 tax forms containing Social Security numbers and other personally identifiable information [view related post]. While the scam has taken different forms, the most prevalent approach is a purported internal email from a company's CEO or CFO to his/her payroll and/or human resource employees requesting all issued W-2s.

While the IRS warning noted that the scam already resulted in "several victims," the phishing efforts are, unfortunately, working on a much larger scale. The director of Experian's data breach resolution group stated earlier this month that the information services company is handling more than 70 data breaches a week resulting from this one type of phishing scam. Perhaps this number is not too surprising when one considers the 100 billion spam emails sent daily.

Incidents of employee negligence continue to be one of the primary causes of data breaches suffered by companies both big and small. Companies may want to strongly consider implementing proactive measures designed at reducing the likelihood of breaches. This could include appropriate training, monitoring, and advising of employees of recent phishing trends and installing appropriate software designed to block spam emails before they hit employee inboxes. Businesses may also contemplate establishing programs designed to reward employees who report potential attacks as opposed to punishing employees who mistakenly respond to a phishing email.

— Brian J. Wheelin

44,000 FDIC Customers' Data "Inadvertently" Taken by Former Employee

In a memo outlining a security incident, as required by the Federal Information Security Modernization Act of 2014, the FDIC has admitted that the data of 44,000 FDIC customers was "inadvertently" taken by an employee as the employee was leaving the employment of the agency.

According to the memo, the employee downloaded the information of the 44,000 customers onto a personal storage device "inadvertently."

According to the FDIC, its "investigation does not indicate that any sensitive information has been disseminated or compromised."

Nonetheless, this incident is a reminder to organizations to keep a close eye on current and departing employees' use of storage devices, including USBs and CDs, which can store large amounts of information. Many companies use technology tools to detect the use of portable devices and prohibit downloading any material to such devices.

— Linn Foster Freedman

DRONES

FAA Committee Report Recommends Operation of Small Drones over Crowds

The Federal Aviation Administration's (FAA) Micro Unmanned Aircraft Systems (UAS) Aviation Rulemaking Committee (ARC) released its "ARC Recommendations Final Report" this month after meeting in March to discuss recommendations for a performance-based standard to "allow for micro UAS to be operated over people who are not directly participating in the operation of the UAS or under a covered structure." ARC considered the risks to the safety of people and property on the ground and in

the air, risks associated with aircraft integrity, and risks associated with crew capability.

ARC's final recommendations consist of a four category system:

- Category 1: Must weigh 250 grams or less; the level of risk of injury posed by this category is so low that no performance standards and no operational restrictions besides the FAA's Part 107 Rule should apply.
- Category 2: Must cause less than a 1 percent chance of injury, must maintain minimum set-off distance of 20 feet above people's heads or 10 feet away laterally, and may not operate so close to people to create an undue hazard.
- Category 3: Must cause less than a 30 percent chance of injury, and may operate over people if:
    - the operation is conducted over a close or restricted access work site with permission of the site owner or operator or
    - overflight of people if they are transient or incidental to the operation of the drone.
- Category 4: Must cause less than a 30 percent chance of injury, and the operation must be conducted in compliance with a documented, risk mitigation plan, which was developed and adopted in accordance with industry consensus.

The standards that apply to Category 2 also apply to Category 3 and Category 4. The ARC report can be accessed in full here. For Categories 2, 3, and 4, there are additional, specific performance standards and manufacturer certifications.

The report also recommends that the FAA change airman certification requirements to allow for online testing to satisfy knowledge requirements and to work to eliminate in-person visits and background checks. The FAA will review these recommendations and offer a period for public comment.

— Kathryn M. Rattigan

ENFORCEMENT + LITIGATION

21st Century Oncology Data Breach Litigation Update

We previously reported that 21st Century Oncology suffered a data breach affecting 2.2 million patients and has been sued in at least two class action lawsuits following notification to the patient [view related posts here and here].

An update on the litigation is that, as of this writing, seven different class action suits have been filed against the Florida company. As with other class action data breach cases, we anticipate that they will be consolidated and will face a motion to dismiss.

We will follow the litigation as it proceeds and keep you updated.

— Linn Foster Freedman

Sony Settles Employees' Class Action Suit for up to $8 Million

The Sony data breach in 2014 was one of the most significant breaches experienced and was a first on many fronts. It was alleged to have been caused by North Korean hackers (calling themselves Guardians of Peace) seeking to disrupt the release of the movie "The Interview," which did not look kindly on North

Korean leader Kim Jong-Un.

The hack caused substantial damage to Sony's computer system and data and the release of confidential emails reverberated throughout the entertainment industry. The intrusion also included access to and posting of the personal information of Sony's employees online.

As a result of the hacking incident, Sony employees filed a class action lawsuit against Sony, alleging poor security practices that resulted in the release of their personal information. The class included 437,000 certified class members. Although the settlement was announced last fall, it was approved by a federal judge in California last week.

The terms of the settlement include up to $10,000 per individual who suffered identity theft losses, plus $1,000-$3,000 for the initial named plaintiffs; identity theft protection services for the class members through 2017; and a fund to compensate members who paid for their own credit monitoring following the breach. And on top of that, the settlement includes $3.4 million for the attorneys.

— Linn Foster Freedman

DATA SECURITY

Feds Identify Security Vulnerabilities in State Health Care Exchange Websites

A Government Accountability Office (GAO) examination of the state-run health insurance exchanges for California, Kentucky, and Vermont identified that there are inadequate security measures in place to protect consumers' personal information. While state officials from Kentucky and California denied that any security breaches had occurred or that any personal data had been compromised as a result of the security weaknesses, state officials acknowledged that several of the flaws have not yet been remedied. Accordingly, the GAO has recommended that the federal government monitor cybersecurity measures on the state-run sites on an ongoing basis.

The GAO examination, which covered the time period from October 2013 to March 2015, identified several basic security flaws in the systems, including the failure to encrypt passwords, to use filters to block hostile access attempts, and to use proper encryption on servers. The GAO report did not specify which state websites suffered from each problem.

Although state officials were notified of the GAO findings in September 2015, responses by state officials from California and Kentucky made clear that not all of the problems had yet been addressed. Officials from Vermont declined to respond to the findings. Due to expenses, Kentucky is in the process of dismantling its state-run exchange and will be transferring to the federal exchange, Healthcare.gov, later this year.

— Benjamin C. Jensen

WhatsApp Adds End-to-End Encryption

More than a billion people on the planet use the online messaging service WhatsApp to send and receive messages, photos and videos and to make phone calls over the Internet. Most of WhatsApp's users are outside the United States.

A subsidiary of Facebook since 2014, WhatsApp just announced the addition of end-to-end encryption to every form of communication on its service. This means all of your messages, phone calls, photos, and videos sent or received over WhatsApp are encrypted. It also means that, if the WhatsApp service is running on your phone, your phone is also encrypted.

End-to-end encryption makes the service secure from hackers and other third parties. In addition, the encryption prevents even WhatsApp employees from accessing your data sent over the service.

Law enforcement has stated that the encryption security makes the service popular with criminals and terrorists. The end-to-end encryption means WhatsApp cannot comply with a court order to provide law enforcement access to your messages, phone calls, photos, or video content. In at least one current case, which remains under seal, WhatsApp maintains it is unable to comply with a federal judge's order to wiretap for a WhatsApp user.

Many lawmakers have called for companies like WhatsApp to equip their encryption schemes with a backdoor available only to law enforcement. Some lawmakers seek legislation requiring back doors. The FBI and the Justice Department maintain they are only trying to keep the status quo—to be able to wiretap a phone call or email with a warrant in hand.

— Kathleen M. Porter

Council of European Union and the European Parliament Approve General Data Protection Regulation; U.S. Privacy Shield Faces Criticism from Article 29 Working Group

The General Data Protection Regulation (GDPR) was recently approved by the 28 member states of the Council of European Union. By plenary vote, the European Parliament approved GDPR on April 14. The GDPR will take effect two years after publication in the E.U. Official Journal, which is expected to be in May.

The GDPR, which strengthens and updates privacy protections for E.U. citizens, has been three years in the making. Many hope it will create a standard for privacy protection across the E.U. rather than the patchwork of member state laws that exist today even beyond the existing E.U. privacy directive, known as Directive 95/46/EC. For the two-year period until the GDPR takes effect, the E.U. will transition from Directive 95/46/EC into GDPR.

Meanwhile, although the European Commission issued an initial decision finding the U.S. Privacy Shield adequate to protect the privacy of E.U. citizens, more recently, a group of E.U. privacy regulators known as the Article 29 group recently expressed their opinion that Privacy Shield failed to adequately protect the mass collection of E.U. citizens' data from U.S. government surveillance. The Article 29 working group also expressed concerns about whether the U.S. ombudsman, will have the power and independence from the U.S. government to hear and manage complaints from European officials, businesses, and individuals.

The Article 29 Working Group's opinion is expected to be considered by national data regulators within each member state and by the European Commission.

— Kathleen M. Porter

PRIVACY TIP #30

Protect Yourself and Your Co-Workers: Please Don't Sell Your Company Credentials

I am on a lot of privacy and security listservs and keep up with surveys relating to data privacy and security. I was most distressed this week to download SailPoint's 2016 Market Pulse Survey. Not that it isn't well done—no—it is quite well done. But the results are really distressing.

The title of the survey is "2016 Market Pulse Survey: Weak Security Practices Leave Organizations Exposed." Isn't that the truth. You can download the survey if you give them your contact information so they can send you marketing materials.

The survey outlines what most of us know: employees continue to be one of the biggest risks to company's data security. Specifically, the report concludes that:

- "Poor password hygiene and negligence continue to plague the enterprise."
- "Data breaches became personal."
- "Organizations are struggling to keep up, and are exposed in the meantime."

The most distressing conclusion? "One in five employees would sell their passwords to an outsider." And they will sell it for peanuts. 44 percent of U.S. employees indicated that they would sell their passwords for less than $1,000. SailPoint says, "Even more concerning? Some would sell their corporate credentials for less than $100."

This, despite the fact that 84 percent of U.S. employees surveyed are concerned that their sensitive information is being shared with others. Apparently they have every right to be concerned when co-workers are so willing to sell their corporate credentials.

News flash to those employees so willing to take cash for corporate credentials—when you give your credentials to someone else, THEY HAVE ACCESS TO AND ARE STEALING YOUR INFORMATION TOO. If you are so concerned about your own information, then keep those credentials secure. And by the way—think about your co-workers and the loss of their data because you sold the keys to the server.

Please, keep your day job and protect your information, your co-workers' information, and your company's information. It's just not worth the $100.

— Linn Foster Freedman
