Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

September 22, 2016

CYBERSECURITY

Survey Shows Employees Top Security Risk for Companies

A recent survey conducted by Arlington Research for OneLogin in May 2016 of 1,022 respondents found what most of us already know: employees continue to be a high risk for employers when it comes to security risk.

The survey shows that although companies are investing in ways to protect their data, cyber-attackers are getting access to company data through employees' digital device practices.

The results of the survey show that 13 percent of U.S. employees allow colleagues to use their company assigned device, even though the employee using the device does not have the same access control, which negates the company's ability to assign access controls based on roles of employees in the company.

Further, nine percent of the respondents allow their spouse/partner to use their company issued device, and one percent allow their children to use their work issued device.

On top of that, the survey confirms that employees frequently share their passwords with their colleagues and 12 percent share their passwords to other work applications, even though there are company policies against this behavior. Not surprisingly, the survey showed that almost 50 percent of the respondents were unaware of their company's policy around sharing passwords.

Finally, the survey comments on how mobile device security is still a risk and is "lax."

The following are some suggestions to combat the risks outlined in the survey:

- Educate employees on the risks associated with sharing passwords and allowing colleagues and unauthorized individuals access to company data
- Implement multifactor authentication
- Consider implementing a BYOD program
- Develop security policies that are easy to understand and user friendly and give real life examples
- Train, educate, re-train and re-educate your employees—and consider doing live education as computer training is pretty boring
- Assemble a data privacy and security team to develop continuous education and awareness for your employees so it is interesting, timely and understandable—the more you reiterate certain behaviors, the more they'll hear the message and perhaps change their behavior—one-time

training is easily forgotten

Most employees really do want to follow company policies, but reading company policies are boring. The key is to find a way to keep employees engaged and part of the solution in data protection.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Judge Approves LifeLock's $68 Million Proposed Settlement with Class and $10.2 Million with Lawyers

On Tuesday, September 20, 2016, a federal judge in California granted approval of the $68 million settlement between LifeLock and a class of plaintiffs that alleged it made false statements about the services it provides to consumers that it will alert them of possible identity theft as soon as possible. The judge also approved a fee of an additional $10.2 million for the lawyers. The settlement funds will come from the $100 million settlement LifeLock reached earlier with the Federal Trade Commission (FTC) last year [view related post]. The FTC alleged that LifeLock had failed to establish a comprehensive information security program and "falsely advertising that it protected consumers' sensitive data with the same high-level safeguards as financial institutions."

The judge rejected several of the plaintiffs' claims that the settlement amount was too low and that the consumers should be reimbursed for the actual amounts paid to LifeLock. One named plaintiff immediately appealed the Order approving the settlement saying the settlement funds should not come out of the FTC settlement and that the attorneys' fees were too high, since the FTC had done most of the work. The attorneys' fees granted by the judge will not be paid out of the settlement with the FTC.

The settlement was reached through mediation, and the consumers in the class will each get $20.

— Linn Foster Freedman

Attorneys Cannot Sue Avvo for Unauthorized Profiles According to Illinois Federal Court

An Illinois federal judge dismissed a proposed class action of lawyers whose business information was published by the online attorney database Avvo without their permission. The lead plaintiff, a Chicago-based personal injury lawyer, claimed that Avvo's service violates the Illinois Right of Publicity Act.

Avvo is designated to permit users to search for attorneys by location, practice area, and other criteria. The company generates revenues by offering attorneys the opportunity to purchase advertising space on competitors' profiles or to ensure that others lawyers cannot promote on their profile.

In granting Avvo's motion to dismiss, the Court relied on the First Amendment protection of publishing truthful newsworthy information. The decision compared Avvo's business model to traditional newspapers that advertise space or a yellow pages directory where businesses can pay for a more prominent listing.

The lead plaintiff argued that Avvo, by selling advertising space through "sponsored" links, was participating in commercial speech. In support of this argument, counsel relied on a recent Seventh Circuit decision in a dispute between basketball icon Michael Jordan and Jewel Food Stores. In that case, Jordan sued Jewel when the grocery chain, without his permission, published an advertisement in a *Sports Illustrated* commemorative issue regarding Jordan's induction into the Hall of Fame that featured

Jordan's basketball sneakers. The Seventh Circuit held that Jewel was not entitled to First Amendment protection since it was promoting its own brand.

The lead plaintiff argued Avvo was similar to Jewel. The Court disagreed noting that Avvo was more akin to Sports Illustrated, who merely published the advertisement.

Last month, Avvo avoided a similar suit in California after the lead plaintiff agreed to withdraw the case and pay Avvo's attorneys fees after the company claimed the litigation violated California's anti-censorship statute.

— Brian J. Wheelin

Employee's Wife Pleads Guilty to Charges After He Stole Patient Information

The Manhattan District Attorney announced this week that the wife of a former employee of Lenox Hill Hospital plead guilty to grand larceny, identity theft in the first degree, and criminal possession of stolen property after her husband stole over 80 patients' information while employed at the hospital. He gave it to her, and she then used the information to access the patients' bank accounts and buy hundreds of thousands of dollars of designer merchandise.

According to the DA, the accused's husband, who had access to patients' names, dates of birth, and Social Security numbers, gave the information to his wife, who used the patients' credit card accounts to place fraudulent telephone orders. In some cases, she was able to obtain account information directly from the card holders' customer service representatives, since she had authentication information.

The DA further alleged that in one instance, she took over a deceased patients' account just hours after the patient passed away.

All in all, she was able to purchase over $300,000 of luxury merchandise and attempted to purchase over $1 million from Saks Fifth Avenue.

Her husband, was fired from Lenox Hill Hospital was fired and subsequently convicted of attempted grand larceny. The DA praised the Hospital on its assistance with the investigation, shutting down the scheme, and bringing it to the DA's attention.

Sentencing is scheduled for October 13, 2016.

— Linn Foster Freedman

DATA BREACH

Yuba Sutter Medical Center Hit with Ransomware

Yuba Sutter Medical Center in California (Yuba Sutter) has notified its patients of a recent ransomware attack that caused parts of its network to be incapacitated. As a result, patient files were unable to be accessed and patient treatment was delayed.

The attack occurred on August 3, 2016. Clinical data and health information was encrypted and the data was backed up. Although patient treatment may have been delayed, it does not appear from reports that

Yuba Sutter paid a ransom.

Patients affected by the ransomware are being notified of the incident. The compromised data includes names, billing information, insurance details, addresses, and telephone numbers.

Yuba Sutter is recommending that its patients watch for suspicious activity on accounts, to obtain a credit report and place a fraud alert with the credit bureaus.

— Linn Foster Freedman

DRONES

Integrating Drones into Your Business

Drones are becoming increasingly important for business of all types and sizes. There are already many applications of drones for businesses, but many more will certainly arise over the next few years. To most effectively and efficiently launch drone operations, here are a few tips on integrating drones into your business:

1. Use Drones to Increase Value. Drones are only as valuable as what they can achieve for your business. Before investing in drones, pilots, and analysis software, create a clear plan for the advantages that drones can provide your business. For example, if your business is large and complex, drones can provide value to the supply chain, inventory management, data gathering, infrastructure inspections, and modelling and mapping. But if your business is smaller, start small.
2. Educate your Business. Drones are frequently in the media these days–mostly for the problems they are causing. While there are certainly risks associated with drone operations, and regulatory requirements, drones can certainly be a value-add to your business. Do the research and prepare reports on how drones can help solve your business's problems and provide your business with third party studies and reports about the same. The more you know about drones and drone operations will only benefit your business.
3. Include Risk Managers and Legal Team in Drone Decisions. Risk management team members and legal counsel are at your business to help prevent accidents and reduce liability. Meet with your risk managers and legal team when considering how your business can integrate drones to benefit the business.
4. Compliance and Operational Efficiency Go Hand-in-Hand. Businesses that invest in commercial drone operations must not only use drones to achieve business value but, must also comply with Federal Aviation Administration (FAA) regulations and state laws as well. Compliance with regulatory requirements and drone operations should be part of one consistent workflow. Hired pilots should understand and abide by the rules and regulations every time.
5. Try More than One Drone and More than One Drone Data Software. While drone aircrafts and data collection software are certainly advanced, there are many different types of aircrafts and software available to choose from. Be sure to shop around for the appropriate drone and software for your business. Use your business's goals to find the right fit.
6. Don't Silo Drone Operations. Depending on the complexity of your business (i.e., the number of departments/divisions, number of jurisdictions in which you operate), there may be a dozen use cases for drones, or even possibly hundreds of flights across the country. Be sure to encourage various departments/divisions in your business to operate on the same set of standards to reduce risks and create transparent drone operations across the business.

— Kathryn M. Rattigan

FINANCIAL SERVICES

The (Regulated) Rise of the CISO

The proposed New York Department of Financial Services Cybersecurity Requirements for Financial Institutions (Regulation) has many different aspects that are designed to bring about overall improvement in cybersecurity programs. One that has yet to be explored is how the Regulation elevates the role of the Chief Information Security Officer (CISO) beyond the traditional role at many financial services companies. The Regulation has detailed requirements for what must be included in a company's cybersecurity policy and procedures. While most of the requirements are standard for information security policies, a few place responsibilities for areas of business that are necessary for cybersecurity, but go far beyond cybersecurity within organizations.

One of the requirements is for inclusion of data governance and classification. Data must be appropriately classified and governance rules applied for proper cybersecurity. However, data classification includes many topics, such as licensed data, third party confidential information, company confidential information, intellectual property, and many others. Data governance ensures that data, when correctly classified, is used in a manner appropriate to the business need, objectives, and in compliance with laws and regulations.

The Regulation also requires business continuity and disaster recovery planning and resources be a part of the cybersecurity policy and procedures. In many companies, the executive responsible for these areas and resources does not report to the CISO. Business continuity and disaster recovery planning also goes far beyond traditional cybersecurity planning and yet, is critical to cybersecurity effectiveness.

Customer data privacy (although interestingly, not employee data privacy) is also required to be included in the cybersecurity policy. Many companies have a Chief Privacy Officer who has operations, policies, and procedures separate from the CISO. The Regulation conflates these areas.

The same applies to physical security and environmental controls, and vendor and third party service provider management. These are operations that are also critical to cybersecurity and yet, the functions have much broader responsibilities. At some institutions, they are well connected. At others, they are not. The Regulation seems to take the position that cybersecurity risk management in these areas is primary.

Perhaps of farthest reach is the requirement for capacity and performance planning to be included in the cybersecurity plan. These are usually the purview of the Chief Information Officer, to whom the CISO often reports. Appropriate operations of systems is critical to protecting the availability and integrity of IT systems. It is also required for the technical operations of the entire enterprise.

The Regulation not only requires financial institutions to focus more explicitly on the cybersecurity program, it also appears to require the elevation of the CISO in order to appropriately manage a broader set of responsibilities.

— *Richard M. Borden*

PRIVACY TIP #53

Valuable Lesson: Don't Write Down Passwords!

I have been doing a lot of live employee training lately. I really enjoy it, and have been told that it is some of the most entertaining training around. The reason I can get the audience to laugh is because I tell real

stories of ridiculous things people have done that have gotten themselves (or mostly their employers) in deep trouble.

I often advocate that everyone should be using passphrases instead of passwords, including a past Privacy Tip. Passphrases are long enough so they will pass muster with any IT security guy's complex password requirement. They are easier to remember and, most importantly, since people usually can remember them, THEY DON'T WRITE THEM DOWN. Most people really like the idea and try to come up with a good passphrase.

And then I read a recent article that made me shake my head in disappointment.

By now, everyone knows not to write down their passwords, not to put them in their top drawer, and not to have it on a post-it note on the monitor of your work station. People actually chuckle at this—like anyone would ever do that…

And yet, people, yes, employees, still write down their passwords.

I also harp on why it is so important to encrypt laptops. If the laptop is encrypted and it is lost or stolen, there may be a safe harbor from breach notification, so encryption is important for mobile devices, including laptops.

In this particular case, the employee of U.S. HealthWorks had an encrypted laptop—so the employer was doing the right thing when it came to data security for laptops—but the employee wrote down his password, and then actually kept the paper that the password was written on WITH THE LAPTOP! So when the laptop was stolen on July 18, 2016, not only did the thief get the laptop, but the thief hit the jackpot because s/he got the password right along with the laptop and the key to the encrypted data, making the encryption useless.

Unfortunately for the employer, it had to notify the 1,400 patients whose information was contained on the laptop because although it was encrypted, the password was available to the thief in order to access the data.

So my tip for this week is DON'T WRITE DOWN PASSWORDS! Do it for yourself *and* for your employer.

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team members regularly serve as presenters at topic-related seminars and participate on panels that discuss developments in the relevant areas. The following are several upcoming speaking engagements:

- October 11 & 12 – InfoGovCon in Providence, RI (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (Linn F. Freedman)
- November 15 – ABA Webinar: "Assessing the Situation: How to Identify and Evaluate the Cyber and Data Risks that a Contractor Bears" (Linn F. 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.

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

Robinson & Cole LLP