Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

June 16, 2016

CYBERSECURITY

Another Popular Car Broken Into by Security Researchers

We have kept abreast of the security vulnerabilities of cars that have been exposed by various security researchers [view recent posts here, here and here]. This time, researchers are asking Mitsubishi to recall approximately 100,000 Outlander hybrid vehicles, as they were able to hack into the security of the car and remotely turn on and off the alarm system, air conditioning, and heating controls and change the program to charge the battery (and essentially drain it) and control the lights.

It all started when the Outlander of one of the researcher's friends showed up as a wi-fi access point on the researcher's phone. He was curious, so he bought an Outlander and started hacking away.

His research found that the Outlander uses wi-fi to connect the car directly with its owner's smartphone instead of a more secure web-based service that uses a GSM module. According to the researcher, this is less secure and allowed the researcher to disable the alarm and open the door. The rest of the vulnerabilities were discovered, including his ability to easily geolocate the car.

He is calling for Mitsubishi to recall the Outlander and reengineer the system. Mitsubishi is working to diligently investigate the problem.

— Linn Foster Freedman

Raytheon/Ponemon Survey Confirms Companies Wait Until an Event to Hire a Data Security Vendor

The results of a Raytheon-commissioned Ponemon study released on June 7, 2016, shows that at least two-thirds of businesses wait until they have experienced a cyber-attack or data breach to hire and retain security vendors to help.

That statistic is consistent with this writer's experience.

The survey, entitled "Don't Wait: The Evolution of Proactive Threat Hunting," includes responses from 1,784 information security professionals in 19 countries about when they outsource network security activities. It also outlines factors important for success, barriers IT departments experience, and challenges with retaining outside data security vendors.

According to the survey, 56 percent of respondents use managed security services (MSS) and 22

percent said they planned to engage an MSS in the future. 80 percent "view MSS as essential, very important or important to their overall IT security strategy. Further, 57 percent of the respondents said they rely on providers, as they did not have adequate in-house capabilities. Unfortunately, 84 percent of the respondents said that the MSS providers do not offer "proactive hunting services" and 80 percent stated that they need to update their IT strategies.

Other findings include that 54 percent of the respondents stated that their MSS provider found software exploitation more than three months old on their network and that insufficient personnel and lack of expertise are challenges to implement a robust cybersecurity program.

Not surprisingly, the survey shows that 65 percent of the respondents "believe their MSSP leverages insight gained from monitoring a large number of security events from a global customer base: …and more than half say it effectively mitigates the risks after they are identified."

Gaining insight from professionals who are seeing threats and responses through the lens of multiple incidents is insightful and essential to a cybersecurity risk management program. The point of the survey is to show that companies are still slow to outsource data security help until after an event, which is too late.

— Linn Foster Freedman

Wells Fargo Unveils Plan to Better Protect Small Business Customer Account Information

On June 7, Wells Fargo announced a partnership with software firm Xero that ntends to allow small businesses to share bank information without sharing their bank passwords with third parties, such as Quicken, who provides services to the business customers. The small business customers will log into Xero's website using a different account designation and password and select the account information that they want shared with the third party. Wells Fargo's and Xero's servers will use a unique token to allow the customer's bank information to be shared with the third party without the password being shared. Tensions have arisen between some banks and data aggregators used by consumers primarily for aggregation of personal data for budgeting and similar personal uses. Concerns have been raised over the sharing of customer bank passwords and collection by aggregators of more data than is necessary to provide the services. Wells Fargo stated that the partnership with Xero is a blueprint for dealing with other more widely used sites.

— Richard M. Borden

DATA PRIVACY

Connecticut Governor Signs Student Privacy Act Into Law

On June 9, 2016, Governor Dannel Malloy, who continues to show his commitment to data privacy, signed An Act Concerning Student Data Privacy into law, effective October 1, 2016.

The law requires any local or regional board of education in Connecticut to enter into a written contract with any operator of an internet website, online service, or mobile application that is used for school purposes and will have access to student information, records, or student-generated content.

The contractual provisions are specifically enumerated and require that the contractor have appropriate security measures in place to protect the student data; that it will be in compliance with FERPA; that it

does not own the student information; that students and parents will have access to the data held by the contractor; that it will have procedures to follow in the event of an unauthorized access, use, or disclosure of the student information; that the information will be returned or destroyed at the end of the contract; and that the information cannot be used by the contractor for any other purpose than to provide the contracted services.

The new law further requires the local or regional board of education to provide to any student and the student's parent electronic notice of the contract entered into within 5 days after signing the contract.

The operators of the internet website, online service, or mobile application must implement appropriate security measures that "meet or exceed industry standards" and delete any student information if requested by a student, parent, or the local or regional board of education.

Further, the operator is prohibited from the following:

- using, selling, or collecting any student information it has access to for targeted advertising to the student or the student's parent
- collecting, storing, or using student information other than for school purposes
- selling, renting, or trading student information
- disclosing student information except in limited circumstances

Finally, in the event of a security breach that results in the unauthorized release, disclosure, or acquisition of student information that does not include student directory information, the operator must provide notification to the local or regional board of education "without unreasonable delay, but not more than 30 days after such discovery" and must also notify the student and the student's parents.

If the unauthorized access, use, or disclosure includes student directory information, the operator must notify the local or regional board of education and the student and the student's parents within 60 days of discovery.

The law also creates a task force to "study issues relating to student data privacy," which is to be convened no later than October 31, 2016.

— Linn Foster Freedman

HEALTH INFORMATION

HHS Guidance Seeks to Clarify Scope of PSQIA

On May 24, 2016, the Department of Health & Human Services (HHS) issued guidance (Guidance) to health care providers and patient safety organizations (PSOs) in an attempt to clarify the definition of patient safety work product (PSWP) under the Patient Safety and Quality Improvement Act of 2005 and its implementing regulations (collectively, the PSQIA).

The PSQIA provides privilege and confidentiality protections for all information collected or developed by a health care provider that qualifies as PSWP and is reported to a PSO recognized by HHS's Agency for Healthcare Research and Quality. However, questions concerning the specific information eligible to qualify as PSWP, and the circumstances under which such information must be developed and retained to maintain PSWP protection, have led to significant uncertainty regarding the scope of the PSQIA. This uncertainty has been particularly acute at the intersection between mandatory federal and state data health care reporting requirements and providers' interests in limiting disclosure of sensitive health information.

The Guidance addresses the lingering uncertainty by restating the definition of PSWP and providing additional detail on the types of information that can and cannot be protected PSWP. Specifically, the Guidance explains the following:

- The PSQIA is intended to "protect the **additional information created through voluntary patient safety activities**, not to protect records created through providers' mandatory information collection activities";
- The **PSQIA does not shield providers from external reporting obligations** and thus cannot be used to prevent disclosure of records required by external recordkeeping or reporting requirements; and
- **PSWP does not include**:
    - "a patient's medical record, billing and discharge information, or any other original patient or provider information";
    - information "collected, maintained, or developed separately, or exists separately, from a patient safety evaluation system";
    - records mandated by federal or state law requirement or other external obligation; or
    - copies of records prepared to satisfy external reporting obligations, even if held inside a provider's patient safety evaluation system.

Although compliance with the PSQIA is completely voluntary, providers seeking to avail themselves of the PSQIA's broad confidentiality and privilege protections would be well-advised to closely review the Guidance to ensure continued compliance with the PSQIA as well as federal and state health care reporting obligations.

— Connor O. Duffy

DRONES

Drone Experts Say Human and Machine Should Be Treated the Same When it Comes to Privacy and Security

Last week, I attended the International Conference on Unmanned Aircraft Systems (ICUAS) in Arlington, Virginia. An ethics and engineering panel set forth some interesting questions for those individuals and businesses interested in becoming part of the drone community. However, as more and more drones hit the skies, more and more privacy and security concerns arise. To bridge that gap, a speaker at the conference from the American Civil Liberties Union (ACLU) suggested using the "privacy by design" concept (i.e., "an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures. That means building in privacy up front—right into the design specifications and architecture of new systems and processes"). Creating drones and UAS that have the ability to create audit logs (e.g., who viewed video/photos from the drone and how many times they viewed it), automatically blur individual faces (e.g., geological surveying recognizing individual people is irrelevant to the mission), use real-time destruction of frames with individuals in the frames), and built-in geo fencing hardwired into the technology will help to alleviate some of the privacy and security concerns associated with drone operations. Moreover, formalized ethics courses to inform engineers about the privacy and security issues is also important.

And why should businesses care about drones and the privacy and security issues related to this technology? Well, there are many nonmilitary uses for UAS—here is just a short list:

- Agriculture, fishery, forestry

- Audio-visual, media, advertising
- Broadcasting and journalism
- Cinema industry
- Construction and real estate
- Environmental (i.e., protection, conservation)
- Heritage and historical monuments
- Humanitarian relief
- Industrial (commercial and corporate)
- Insurance (investigations)
- Maintenance
- Mining and exploration
- Policy compliance and legal proof
- Public safety (i.e., animal deterrent, civil protection, disaster management, fire fighting, pubic gatherings, critical installations)
- Public security and law enforcement (i.e., police, border control, coast guard, customs, gamekeeping, judiciary)
- Research and scientific
- Utility companies
- Training and instruction

We can use UAS to advertise, broadcast, and shoot film for movies and television; deter animals on farmland; dispense food and medicine, explore, inspect, map, measure, monitor, observe, patrol, and conduct relief flights; research; conduct search and rescue; spray, survey, test, and track; and use for water bombing. We just want to be sure that we build privacy and security into drones and UAS from the beginning, so we can use this technology safely, efficiently, and effectively without invading individual privacy rights.

— Kathryn M. Rattigan

First Company in the World to Create Drone Navigation System Integrated with Insurance

Last week, Singapore-based ALAS Pte Ltd (ALAS) demonstrated its new software system for drone navigation, integrated with insurance for all users, at the Asia Pacific Remotely Piloted Aircraft Systems (RPAS) Symposium held in Singapore.

ALAS stands for "Airspace Localization and Avoidance System" this system has the ability to make multiple autonomous drone flights safely and effectively. The plan is to work with insurance companies to offer inexpensive insurance packages that come with the ALAS software.

ALAS Chief Technology Officer Dr. Jaime Rubio Hervas described software system as “WAZE in the Sky” (WAZE is a popular road navigation app). ALAS, much like WAZE, can offer real-time chats, sharing, and crowd-sourcing information among users, which will greatly increase safe drone operation.

Dr. Hervas said in an interview at the symposium, “After much research, we found that there isn’t a single company which offers both a drone navigation system and insurance coverage, so we decided that we would fill that gap. Although still a work-in-progress, our insurance will be fuss-free. With a simple click-through, users can purchase insurance directly via the software, making it as convenient as possible.” ALAS is intended for use by commercial drone operators, civil aviation regulators, air traffic controllers, insurance companies, private companies, and even members of the general public who wish to be aware of the drone traffic around them. For additional info, check out the ALAS website.

— Kathryn M. Rattigan

Recreational Model Aircraft Hobbyist Files Appeal against FAA for Drone Registration

We previously reported that model aircraft hobbyist John Taylor filed suit against the Federal Aviation Administration (FAA), challenging the requirement to register with the FAA in order to fly his model aircraft near his home. On June 14, 2016, Mr. Taylor filed his appeal to the DC Court of Appeals to "order the FAA to permanently destroy the recreational model aircraft registry and refund registration moneys received."

Mr. Taylor alleges that the FAA issued the Registration and Marking Requirements for Small Unmanned Aircraft on December 16, 2015, without proper notice and comment and requested the federal district court to review the issuance. He has further requested review of the FAA's advisory circular that states that model aircraft must not operate in the DC Special Flight Rules Area, which encompasses a 30-mile radius from Reagan National Airport and review of the establishment of a task force to determine the best approach to registering model aircraft. According to Mr. Taylor, the FAA has "declared the entire Washington, D.C. metropolitan area, and beyond, to be a 'no drone zone…" According to Mr. Taylor's brief, the drone registration requirements "apply to all model aircraft, regardless of size….They apply to a child playing with a small flying toy a few feet off the ground in the family's back yard."

We will continue to watch this case, and the challenge to the FAA's drone registration requirements, closely and continue to report on developments as they unfold.

— Linn Foster Freedman

DATA BREACH

Government Report Critiques the IRS's Handling of 2015 Data Breach

According to a government report publicly released last week, the IRS failed to adequately respond to a May 2015 cyber-attack on its "Get Transcript" application that potentially compromised at least 621,000 taxpayer accounts. The United States Treasury Inspector General for Tax Administration (TIGTA) found that, while the IRS timely disabled the affected application, it failed to identify all potential taxpayers affected by the breach. It was only after the TIGTA alerted the IRS of the larger scope of the breach that the IRS informed all affected taxpayers.

The IRS's own figures continually increased over the course of the last year. Days after the breach, the IRS reported that the affected number was approximately 100,000. That figure doubled in August 2015. It then doubled again in February 2016. In a statement, the agency noted that all affected taxpayers were informed as soon as they were identified.

The TIGTA report also critiqued the IRS for failing to offer credit monitoring services to the roughly 79,000 taxpayers where only an attempted access occurred. Given that the breach created an increased risk of false tax returns being filed, the TIGTA noted that all targeted accounts should have received the service. In response, the IRS disagreed with this critique, given that, for these 79,000 taxpayers, there was no evidence that these individuals had any information stolen. However, the IRS did agree with recommendations in the report regarding the content of its notification letters.

The agency also touted the recent unveiling of a more rigorous e-authentication process for its "Get Transcript" application, which has allowed 47 million transcripts to be ordered since its 2014 launch.

— Brian J. Wheelin

PRIVACY TIP #39

Be Wary of IRS Phone Scams

Although the IRS has warned taxpayers on multiple occasions about IRS phone scams, consumers continue to be victims. This lucrative scam, which for years, according to the IRS, has cost victims more than $26 million since 2013, is only getting worse.

The typical IRS phone scam is when someone calls stating that s/he is an IRS agent and that the taxpayer has an IRS tax bill that must be paid immediately and leaves urgent requests for the taxpayer to call back about a tax liability. The phony IRS agent threatens the consumers and tries to scare them into believing they can go to jail, be deported, or have their driver's license revoked if they don't pay the delinquent tax bill.

Phone scamming has been on the rise and will not stop anytime soon. It has become such a problem that last month the IRS issued an internal memo telling all IRS employees to no longer initiate any contact with taxpayers by telephone. This means that IRS officials will not be initiating any telephone calls with taxpayers.

The tip this week? Be wary of anyone who calls, texts, or emails you stating that they are an IRS official and that you owe money. That's NOT how the IRS communicates with taxpayers. The IRS typically provides all notices to taxpayers through the regular mail. If you get a letter from the IRS, pay attention. If you get a phone call, don't respond and don't be the victim of a scam.

— 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 area. Following, are several upcoming speaking engagements:

- June 21 & 22 – Cloud Financial Services USA Conference in New York City (Richard M. Borden)
- June 22 – National Scholarship Providers Association in Rocky Hill, CT (Linn F. Freedman)
- June 23 – MCLE: Data Security 2.0: The Cloud, Mobile Devices & Encryption Webcast Panel (Kathleen M. Porter)
- July 11 & 12 – Seventeenth Annual Institute on Privacy and Data Security Law (Kathleen M. Porter)

- September 12 - 15 – ASIS 2016: 360° VISION in Orlando, FL (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (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.