Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | December 2017

We focus this month on data security, cybersecurity, and some of the implications of security breaches. Megan Brown and Kathleen Scott evaluate potential risks from the operation of Information Sharing and Analysis Centers. Ted Brown reviews an important recent decision involving insurance coverage for a data breach class action. We also include a transcript of my recent interview with the Information Security Media Group concerning how best to work with law enforcement in connection with security breaches. Last, Megan Brown, Kathleen Scott, Madeleine Lottenbach, and Shawn Donovan review the recent release by the National Institute of Standards and Technology (NIST) of the draft update to its cybersecurity framework.

As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

Security Discussions – Are ISACs' Operations Vulnerable to Third Parties?

By Megan L. Brown and Kathleen E. Scott

In 2015, *WIRED* magazine brought public attention to a claimed cybersecurity vulnerability in the entertainment systems of certain vehicles.[1] This software vulnerability allegedly allowed security researchers to hack the vehicles and take control of various elements, from dashboard functions to steering.[2] Following this report, over a million vehicles were recalled,[3] and some owners and lessees of the vehicles initiated class action litigation – *Flynn v. FCA* – over the alleged flaw.[4] While research exposed

ALSO IN THIS ISSUE

[1] Hackers Remotely Kill a Jeep on the Highway (July 21, 2015), *available* **here**.
[2] After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix (July 24, 2015), *available* **here**.
[3] After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix (July 24, 2015), *available* **here**.
[4] *Flynn v. FCA U.S. LLC and Harman International Industries, Inc.*, Case No. 16-mc-00078 DGW (S.D. Cal.).

continued on page 2

‘Data Breach’ Class Action Not Covered Under CGL Policy

By Edward R. Brown

A Florida federal district court, applying South Carolina law, has held that a claim arising out of a data breach alleging that an insured failed to safeguard personal information did not trigger personal and advertising injury coverage under a commercial general liability policy. *Innovak Int’l, Inc. v. The Hanover Ins. Co.*, No. 8:16-cv-2453-MSS-JSS (M.D. Fla. Nov. 17, 2017).

The insured, a software developer, suffered a data breach. As part of that incident, hackers gained access to Social Security numbers, addresses, telephone numbers, dates of birth, and other personal information of a large number of individuals. Later, the insured was sued in a putative class action. It sought coverage under its CGL policy, which afforded coverage for “personal and advertising injury,” defined in relevant part to include “injury … arising out of … [o]ral or written publication, in any manner, of material that violates a person’s right of privacy.” The insurer denied coverage, and the insured brought suit.

In the coverage action, the court granted summary judgment in favor of the insurer. The court ruled that “the only plausible interpretation” of the personal and advertising injury coverage was that “it

continued on page 3

Security Discussions – Are ISACs’ Operations Vulnerable to Third Parties?

continued from page 1

alleged vulnerabilities in entertainment systems, the ongoing litigation has exposed vulnerabilities in the current approach to cybersecurity information sharing and the need for a policy solution.

ISAC Vulnerability

Specifically, in the summer of 2016, the plaintiffs in *Flynn* served a subpoena on the Automotive Information Sharing and Analysis Center (Auto-ISAC) seeking, among other things, communications between the defendant automaker and the non-party ISAC. The ISAC was able to successfully fend off the subpoena. The court ordered the subpoena to be quashed, agreeing with the Auto-ISAC that the subpoenaed documents were not relevant to the underlying case.[5] The subpoena, despite being quashed, reveals real weaknesses in the current U.S. approach to cybersecurity information sharing.

The importance of cybersecurity information sharing cannot be overstated. Industry needs to be able to share information about threats and countermeasures, among other things, with each other and with government to effectively combat the ever-evolving threat landscape. Robust legal protections are needed to ensure that companies can voluntarily engage actively in real-time sharing without the threat of liability. Congress recognized this and passed the Cybersecurity Information Sharing Act of

continued on page 3

[5] *Flynn v. FCA and Harman International Industries, Inc.*, Order, Case No. 16-mc-00078 DGW, at 6 (S.D. Cal. Nov. 30, 2016).
[6] Pub. L. 114-113, 6 U.S.C. § 1501.

Security Discussions – Are ISACs' Operations Vulnerable to Third Parties?

continued from page 2

2015 (CISA), which promotes and protects voluntary information sharing.[6]

ISACs are important venues for information sharing. The idea for sector-specific ISACs formed in the late 1990s,[7] and today, there are more than 20 sector-based ISACs serving as information-sharing hubs for critical infrastructure industries ranging from the automobile industry (Auto-ISAC) to the communications industry (COMM-ISAC). These organizations "collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency"; they also coordinate across sectors.[8]

However, despite federal policy to promote voluntary information sharing – from CISA and through the ISAC infrastructure – there remain risks associated with information sharing, as highlighted in *Flynn*. There is little to stop another set of plaintiffs in another class action lawsuit from seeking communications between companies and their ISAC, and another court may reach a different conclusion than the *Flynn* court did.

The Resulting Risk

The mere suggestion that communications with information-sharing organizations are not protectable may have a chilling effect on companies' willingness to share information. This outcome is unacceptable, given the critical importance of cybersecurity and information sharing. Policymakers should work with urgency to fully protect entities involved in cybersecurity information sharing, and ensure that all cyber communications remain protected. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

[7] *See* **here**.
[5] National Council of ISACs. *See* **here**.

'Data Breach' Class Action Not Covered Under CGL Policy

continued from page 2

requires the insured to be the publisher" of the sensitive material. Here, the insured was alleged to have been passively negligent in failing to safeguard information. The court also ruled that even if "indirect publication" by the insured would be sufficient to trigger coverage, there had been no publication at all, and the mere fact that hackers obtained information was not a proxy for finding "publication."

Innovak underscores that companies should not generally rely on traditional CGL insurance to cover "cyber"-related risks. Instead, along with technical safeguards, vendor due diligence, and appropriate contractual mechanisms, organizations should purchase specialized "cyber" coverage to manage their risks for these growing exposures. "Cyber" insurance, both for first-party and third-party coverages, is widely available in the marketplace and increasingly purchased by organizations of all types and sizes. ■

For more information, please contact:

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Reporting Breaches to Law Enforcement: Why Timing Matters

Kirk Nahra recently was interviewed by Marianne Kolbasuk McGee, executive editor at the Information Security Media Group, concerning the important topic of reporting breaches to law enforcement.

Marianne Kolbasuk McGee: Organizations that have suffered a breach sometimes wonder whether or not they need to report it to law enforcement. When should they figure this out and typically what kind of breaches need to be reported?

Kirk Nahra: Those are tricky questions, something that is obviously affecting a lot of companies and there has been an evolution in thinking over the last few years. I think a lot of companies originally didn't want to go to law enforcement or didn't think to go to law enforcement, although that depended a little bit on the kind of breach. If it was an employee who did something, a lost piece of information, a lost laptop or something like that, your first instinct was not necessarily to go to law enforcement. People started by focusing on notice as a regulatory issue and as a consumer issue; they didn't really think about law enforcement as something that could help in connection with the situation. Now, particularly with some more advanced kinds of breaches, whether it's a hacking incident or ransomware or something like that, law enforcement can really help deal with the breach, help you try to mitigate the problems. They are not the regulators for the most part; they are separate from the regulators, and they do not usually share a lot of information with the regulators, so often they can be very helpful.

Marianne Kolbasuk McGee: Do you find that health organizations are more willing to go to law enforcement if it was a cyberattack by the big bad wolf, as opposed to somebody in their organization that did something, because that's more embarrassing?

Kirk Nahra: I think embarrassment is a factor, but I'm not sure that is the driving force. I think a lot of times the company's sense is that they can deal with it themselves. A lot of times what you have to also think about are the timing issues. A lot of times you're trying to deal with an issue right away, and the first instinct, if it is an employee situation, is to try to deal with it as an employee issue. There may come a point in time once you learn some more facts where you want to report something to law enforcement, but I think for employee situations, law enforcement often hasn't been the first instinct of companies, and I can't even say that's wrong necessarily. I think there are other situations, and maybe a hacking incident or a ransomware would be good examples of that, where it's clearly not something that's internal, it's not something that most companies have any real expertise in being able to deal with, and it's something where the skills of law enforcement can really perhaps be helpful. Bringing law enforcement in doesn't mean you are going to solve the problem, but it gives you a better chance in a lot of situations.

Marianne Kolbasuk McGee: Law enforcement can be helpful, but does it slow things down, like "you can't do this, or can't fix that because we need the evidence"?

Kirk Nahra: Yes, how you work with law enforcement on timing is a part of the puzzle that you have to deal with if you are a company. Your obligations as the company don't necessarily slow down because law

continued on page 5

enforcement is involved. They can, in certain situations where law enforcement may say "we don't want you to do something," but that's usually not the case. And so often companies have to conduct their own kinds of investigations to try to figure out what their obligations are in connection with their other requirements – whether they have to notify a specific regulator, whether they have to notify individuals, whether they have to notify their own business partners. And government's, or law enforcement's, speed or lack of speed on that is really an independent variable. So law enforcement may eventually still be helpful, if they want to prosecute somebody, if they want to recover lost assets, but for those immediate challenges, it may be that law enforcement, even if they work diligently, can't really do anything to affect your timing on that. So you always have to factor that in, which is why you don't hand it over to law enforcement. You try to help work with law enforcement as one component of your overall response to the breach situation.

Marianne Kolbasuk McGee: Do you see any organizations hesitating to report things to law enforcement because they are not sure if it really is a reportable breach, and they are afraid that once law enforcement hears about it, so does the Office for Civil Rights?

Kirk Nahra: There are a couple of points there. I think there is clearly a tension between your regulatory reporting obligations and when it makes sense to use law enforcement. I don't think that reporting an event to law enforcement automatically makes it more or less likely that OCR is going to know anything about it, but again it's an independent variable. The idea in most breach situations is it's a breach that requires reporting unless you can prove it's not a breach that requires reporting. If it's an unknown situation, that's where the regulatory guidance comes in and most companies are going to feel a need to report it to OCR, which also means to the consumers, and really it's consumers first and then maybe OCR in connection with the individual reporting. But you have to go down that path regardless of what law enforcement is doing. Again, there certainly are companies who may say, I don't think this is a big deal or the ransomware has not been put on our patient records, it's been put on our medical research records or our corporate financial information or something that's not likely to be protected health information and not likely to trigger some of the regulatory obligations. But again, you have to sort of deal with those in parallel, and that's where a good, smart in-house counsel or outside lawyers can help you navigate that and work through all of those variables in connection with a single incident, often at a very quick pace. ■

For more information on use of law enforcement and other breach response challenges, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

The interview was originally published on Information Security Media Group's HealthcareInfoSecurity.com news website on December 4, 2017.

continued on page 7

NIST Releases Draft 2 of Its Cybersecurity Framework Version 1.1

By Megan L. Brown, Kathleen E. Scott, Madeleine M. Lottenbach, and Shawn M. Donovan

On December 5, 2017, the National Institute of Standards and Technology (NIST) released the much-anticipated second draft of its Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Framework Version 1.1 Draft 2 or Draft 2), along with a draft companion Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1 (Roadmap) and a Fact Sheet detailing its changes and process.

Draft 2 is intended to reflect the feedback that NIST received from stakeholders regarding Framework Version 1.1 Draft 1 (Draft 1), which was originally released in January 2017. The new Draft 2 makes significant changes to the section on cybersecurity measurements, in line with stakeholder feedback. Public comments on Framework Version 1.1 Draft 2 are due January 19, 2018. NIST intends to publish the final Framework Version 1.1 in early 2018.

NIST originally published the Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (Framework Version 1.0) in February 2014. As NIST describes, the Framework is voluntary guidance for critical infrastructure organizations. It is based on existing standards, guidelines, and practices, and intends to help organizations to better manage and reduce cybersecurity risk and to foster risk and cybersecurity management communications.

The Framework Version 1.1 is meant to refine, clarify, and enhance the Framework Version 1.0. With this update, NIST is striving to cause as little disruption to implementation of the Framework as possible – meaning that current users of the Framework Version 1.0 should be able to easily implement Framework Version 1.1.

Key Updates

Draft 2 makes several key updates to Draft 1, including:

- Cybersecurity Measurements: NIST revises its new section on cybersecurity measurements significantly. It truncates the discussion, cutting it from four pages in Draft 1 to just over one page in Draft 2. It also changes the title of the section from “Measuring and Demonstrating Cybersecurity” to “Self-Assessing Cybersecurity Risk with the Framework” and emphasizes that self-assessments are linked to organizational objectives, highlighting flexibility and customization.

- Supply Chain Risk Management: NIST refines its addition of Supply Chain Risk Management (SCRM) from Draft 1, clarifying the section on communicating risks with stakeholders and incorporating that information into the Implementation Tiers.

- Authorization, Authentication, and Identity Proofing: NIST adds a new authentication subcategory and provides a number of authentication Informative References. Draft 2 further highlights authentication in the document, adding a reference to authentication in the Privacy and Civil Liberties section.

- Coordinated Vulnerability Disclosures: NIST adds a new subcategory regarding internal and external vulnerability disclosure programs. It also provides

NIST Releases Draft 2 of Its Cybersecurity Framework Version 1.1

continued from page 6

a number of vulnerability disclosure Informative References.

- Federal Alignment: Draft 1 had added a section detailing requirements of federal information systems. However, NIST removes that section in Draft 2, explaining that such statements are covered by other documents – including NISTIR 8170 – and therefore are not needed in the Framework.
- Application to the Internet of Things: NIST updates the scope of technologies covered by the Framework to "reflect security implications of a broadening use of technology." Draft 2 notes that members of each critical infrastructure sector perform functions supported by broad categories of technology, "including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT)." While CPS was added in Draft 1, the application to IoT devices in Draft 2 is new.

"Roadmap" Updates

In addition to the updates to the Framework Version 1.1, NIST also published a draft update to the Framework's companion Roadmap. NIST first published a companion Framework Version 1.0 Roadmap in 2014. Like that document, the newly published draft "provides a description of anticipated future activities related to the Framework and offers stakeholders another opportunity to participate actively in the continuing Framework development process." Updates to the Roadmap for Version 1.1 include:

- Cyber-Attack Lifecycle
- Measuring Cybersecurity
- Referencing Techniques
- Small Business Awareness and Resources
- Governance and Enterprise Risk Management

NIST also has renamed several sections in the new Roadmap draft:

- "Authentication" has been renamed to be "Identity Management" to cover a broader range of technical topics.
- "Technical Privacy Standards" has been renamed to be "Privacy Engineering," in line with NIST's related Interagency Report 8062 – An Introduction to Privacy Engineering and Risk Management in Federal Systems.
- "Conformance Assessment" has been renamed to be "Confidence Mechanisms" to show a broader range of digital trust activities. ■

For more information on Draft 2 or the NIST process, please contact:

Megan L. Brown
| 202.719.7579
| mbrown@wileyrein.com

Kathleen E. Scott
| 202.719.7577
| kscott@wileyrein.com

Madeleine M. Lottenbach
| 202.719.4193
| mlottenbach@wileyrein.com

Shawn M. Donovan
| 202.719.7293
| sdonovan@wileyrein.com

Events & Speeches

The New Era of Big Data for Health Care

Kirk J. Nahra, Speaker

Physicians and Hospitals Law Institute

February 7, 2018 | New Orleans, LA

Legal and Regulatory Considerations in the U.S. and Internationally

Kirk J. Nahra, Speaker

HITRUST TPA Summit 2018

February 20, 2018 | Chicago, IL

HIPAA 2.0—Building Better Privacy and Security Rules

Kirk J. Nahra, Speaker

IAPP's Global Privacy Summit

March 27, 2018 | Washington, DC

The Path Towards a New and Complete Consumer Health Regulatory Structure

Kirk J. Nahra, Speaker

Twenty-Seventh National HIPAA Summit

March 28, 2018 | Arlington, VA

Privacy and Security Enforcement Highlights

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 2018 | Orlando, FL

Top Ten Privacy and Security Developments for the Health Care Industry

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 2018 | Orlando, FL

Contributing Authors

Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Shawn M. Donovan	202.719.7293	sdonovan@wileyrein.com
Madeleine M. Lottenbach	202.719.4193	mlottenbach@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com

To update your contact information or to cancel your subscription to this newsletter, visit:

www.wileyrein.com/newsroom-signup.html.

This is a publication of Wiley Rein LLP, intended to provide general news about recent legal developments and should not be construed as providing legal advice or legal opinions. You should consult an attorney for any specific legal questions.

Some of the content in this publication may be considered attorney advertising under applicable state laws. Prior results do not guarantee a similar outcome.