Cybersecurity breaches and risk management continue to be a concern for businesses of all sizes and types. A recent warning distributed by the U.S. Department of Homeland Security and the FBI regarding targeted hacks in several critical industries is an illustration that anyone can be vulnerable such tactics, including the hospitality industry. My partner Bob Braun, senior member of JMBM’s Global Hospitality Group® and co-chair of JMBM’s Cybersecurity and Privacy Group, summarizes the recent report and its conclusions below.

Homeland Security Warns Against Threats to US Infrastructure by Robert E. Braun

25 October 2017
Click here for the latest articles on Data Technology, Privacy & Security

Homeland Security Warns Against Threats to US Infrastructure by Robert E. Braun

The Department of Homeland Security and Federal Bureau of Investigation distributed an email warning late on Friday, October 20, 2017, that the nuclear, energy, aviation, water and critical manufacturing industries have been targeted along with government entities in attacks dating back to at least May. In particular, the agencies reported that hackers had compromised some targeted networks, but did not identify specific victims or provide other details.

While the report focused on threats to nuclear and conventional power, water, and other infrastructure, the very fact that the DHS and the FBI chose to make a public statement highlights how important the issue is to all industries, and the concern that an attack on infrastructure could have a devastating impact on all aspects of the American economy.

The report noted that, as in many malware attacks, hackers seek to compromise networks with “spear phishing” – emails tailored to reach specific individuals – with malicious attachments and tainted websites with a goal of obtaining credentials that allow the hackers to access computer networks.

Attacks on U.S. public infrastructure have been reported in the past, and authorities initially detailed the attempts in a confidential report in June of this year. That document, which was privately distributed to firms at risk of attacks, described a narrower set of activity focusing on the nuclear, energy and critical manufacturing sectors.

Robert Lee, an expert in securing industrial networks and chief executive of cyber-security firm Dragos, said the report appears to describe hackers working in the interests of the Russian government, though he declined to elaborate. Dragos reported that it is also monitoring other groups targeting infrastructure that appear to be aligned with China, Iran and North Korea, he said.

Lee said that the hacking described in the government report is unlikely to result in dramatic attacks in the near term, but
that it is still troubling: “We don’t want our adversaries learning enough to be able to do things that are disruptive later.”

The report said that hackers have succeeded in infiltrating some targets, including at least one energy generator, and conducting reconnaissance on their networks. It was accompanied by six technical documents describing malware used in the attacks.

Homeland Security “has confidence that this campaign is still ongoing and threat actors are actively pursuing their objectives over a long-term campaign,” the report said.

A full copy of the report can be accessed at https://www.us-cert.gov/ncas/alerts/TA17-293A. For additional information on how you can address cybersecurity threats and needs, contact Bob Braun at rbraun@jmbm.com.

JMBM’s Global Hospitality Group® works with the JMBM Cybersecurity and Privacy Group to help clients analyze risk and develop response plans and other procedures to reduce vulnerability to data breaches. For more information, contact Bob Braun at rbraun@jmbm.com.

Other information about cybersecurity issues

If this article was of interest, you may also wish to read other articles on “Data Technology, Privacy & Security,” which include the following articles:

- Hotel Cybersecurity: Protecting your guests and your property from vendor data breaches
- Hotel Cybersecurity: What can happen when hackers strike?
- Hotel Cybersecurity: Closing the doors before the horses leave the barn
- What every hotel owner (and operator) needs to know about “data security” after the Wyndham case
- What the Target data security breaches mean for hoteliers
- Cyber Security Alert: How to protect your proprietary information from employees
- Hotel Lawyer Privacy Alert: Do your hotel mobile apps comply with new interpretations of online privacy rules?
- Hotel Liability for Guest Information — What you need to know and how to avoid liability.
- Losing the expectation of privacy bit by bit, byte by byte.
- Dodd-Frank Act presents Hotels with decisions on credit and debit card charges.
Bob Braun is a Senior Member of JMBM’s Global Hospitality Group® and is Co-Chair of the Firm’s Cybersecurity & Privacy Group. Bob has more than 20 years experience in representing hotel owners and developers in their contracts, relationships and disputes with hotel managers, licensors, franchisors and brands, and has negotiated hundreds of hotel management and franchise agreements. His practice includes experience with virtually every significant hotel brand and manager.

Bob also advises clients on condo hotel securities issues and many transactional matters, including entity formation, financing, and joint ventures, and works with companies on their data technology, privacy and security matters. These include software licensing, cloud computing, e-commerce, data processing and outsourcing agreements for the hospitality industry.

In addition, Bob is a frequent lecturer as an expert in technology, privacy and data security issues, and is one of only two attorneys in the 2015 listing of SuperLawyers to be recognized for expertise in Information Technology. Bob is on the Advisory Board of the Information Systems Security Association, Los Angeles chapter, and a member of the International Association of Privacy Professionals. Contact Bob Braun at 310.785.5331 or rbraun@jmbm.com.

This is Jim Butler, author of www.HotelLawBlog.com and hotel lawyer, signing off. Please contact us if you would like to discuss any issues or development that affect your hotel interests. We would like to see if our experience might help you create value or avoid unnecessary pitfalls. Who’s your hotel lawyer?

Jim Butler is a founding partner of JMBM and JMBM’s Global Hospitality Group® which provides business and legal advice to hotel owners, developers and investors. This advice covers hotel purchase, sale, development, financing, franchise, management, labor & employment, litigation, ADA, IP, EB-5 matters any many other areas.

Jim is recognized as one of the top hotel lawyers in the world and has led the Global Hospitality Group® in more than $71 billion of hotel transactions and more than 3,800 hotel properties located around the globe.

Jim’s group has advised on more than 100 EB-5 projects, closed more than $1.5 billion of EB-5 financing, and sourced more than half of that for our clients.
Contact Jim at +1-310.201-3526 or JButler@jmbm.com