Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Iranian Cyber Threat Raises Stakes For Corporate Security

By **Allison Grande**

Law360 (January 10, 2020, 9:53 PM EST) -- Regulatory warnings about a heightened Iranian hacking threat have put banks, telecoms and other businesses on notice they need to move quickly to ensure basic cybersecurity measures are in place to reduce the chance of being held liable in any attacks, experts say.

On the heels of the U.S. airstrike that killed Iran's top general Jan. 3, the U.S. Department of Homeland Security and New York Department of Financial Services separately flagged Iran's history of launching cyberattacks in the U.S. and cautioned businesses of the increased potential for retaliatory cyber hits by Iranian government-backed hackers. Texas Gov. Greg Abbott also urged residents to be "particularly vigilant" of the mounting Iranian cyberthreat.

"The current warnings serve as a reminder to everyone that these threats are very real, and if they're ignored, it could be very costly," said Nickolas B. Savage, an associate managing director in Kroll's cyber risk practice and a former assistant special agent in charge at the FBI.

The advisories also essentially eliminate the ability for companies — particularly critical infrastructure operators such as banks, internet providers and electric companies — to completely skirt culpability for such attacks by merely pointing to the highly motivated and sophisticated nature of the hackers, experts say.

"With these alerts, it can be said that companies should be reasonably aware that there's a higher degree of risk," said Robert Braun, a partner at Jeffer Mangels Butler & Mitchell LLP and co-chair of the firm's cybersecurity and privacy group. "So if people don't pay attention to them and then something happens, there's going to be an issue."

Companies have faced both internal and external pressure in recent years to shore up their cyber defenses. New data security laws in several U.S. states and abroad have forced businesses to pay closer attention to the data they have and how they're protecting it, and enforcers such as U.S. state attorneys general and European Union data protection authorities have stepped up their oversight and increased the fines for data security missteps.

While nation-state threats such as the one posed by Iran's well-equipped and advanced cyber arsenal may be difficult for companies to avoid altogether, taking basic security steps — such as ensuring that security patches are up to date and that employees are adequately trained about the risks of clicking on

suspicious links and email attachments — could go a long way toward avoiding a hefty fine or an unfavorable judgment in a consumer class action, according to experts.

"No matter where the attack comes from — whether it's from a nation-state or some kid in a basement — companies can be seen as negligent if they don't do the right things to protect the organization from such attacks," said Debbie Gordon, CEO of Cloud Range Cyber.

Companies' regulatory obligations, such as notifying affected individuals of the incident or complying with the payment card industry's data security standards, don't change depending on the source of the attack, attorneys noted.

But what can change from incident to incident is the range of penalties and litigation risk that companies may face, according to April Doss, a partner at Saul Ewing Arnstein & Lehr LLP and former minority counsel for the Senate Select Committee on Intelligence.

When a regulatory body approaches a company post-incident to find out what happened, "if the underlying facts are that the breach happened because a particularly sophisticated nation-state actor was able to carry out a particularly sophisticated attack on a company's network, and the company that suffered the breach did a great many reasonable things expected in the industry to protect the data, then the enforcer would likely look at that and be more likely to not find any fault or culpability on behalf of the company," Doss said.

However, if it's found that a company had failed to take basic cybersecurity steps and that the nation-state hackers had exploited a vulnerability that could have been addressed by these measures, then a regulatory body may be more likely to "look at the company and say maybe they're not living up to its responsibilities here," Doss added.

The advisories therefore provide a golden opportunity for companies to address or revisit the strength of the steps they're taking to protect their network from external threats.

“These warnings put companies on notice that cyber risk is elevated right now and in the near and even the medium term, so if they haven’t been prioritizing cybersecurity, now would be a good time to start,” said Jonathan Meyer, a Sheppard Mullin Richter & Hampton LLP partner and former deputy general counsel at the DHS.

Companies of all sizes are no strangers to cyberthreats. They've long had to be on high alert for cyberattacks orchestrated by both nation-state and independent hackers bent on stealing sensitive personal information or locking down systems in exchange for ransom.

Most attacks have been financially motivated. But over the past decade, another purpose has begun to emerge more fully: to wreak havoc and show power in international conflicts, such as the one exacerbated by the slaying of Iranian Gen. Qasem Soleimani.

"We're continuing to see nation-states, including those that are adversarial to the U.S., use cyber tools as a means of projecting power around the world without having to undertake physical movement of people or troops or engaging in trade wars that might be harmful to them economically," Doss said.

The latest Iranian cyberthreat provides the newest wrinkle, with any attacks likely to be propelled not by a desire to steal money or valuable data, but rather by a drive to sow fear and uncertainty.

"This offensive effort from Iran is going to be about disruption, primarily how to disrupt Americans' daily lives and the country's war-fighting capabilities," said Jordan Mauriello, senior vice president of managed security at cybersecurity firm Critical Start.

The Jan. 4 bulletin issued by DHS' National Terrorism Advisory system noted that "Iran maintains a robust cyber program and can execute cyber attacks against the United States. Iran is capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure in the United States."

Mauriello said that during the past week his firm has "definitely seen an uptick in activity" from Iran, although he noted it wasn't in terms of offensive direct attacks but more related to "reconnaissance and probing activities, preparatory activities, like sending in advance scouts in kinetic warfare."

These findings are consistent with Texas Gov. Abbott's warning Tuesday, in which he disclosed that as many as 10,000 attempted attacks per minute from Iran had been detected over the past 48 hours on state agency networks.

While U.S. officials have stressed that they currently don't have information about any specific or credible threats from Iran, the country's Islamic Revolutionary Guard Corps has a robust cyber unit, and Iranian-sponsored hackers have a history of targeting U.S. critical infrastructure such as banks and the power grid, where a disruption of service could cause the most widespread damage.

U.S. authorities in 2016 charged several Iranian-sponsored individuals with carrying out denial of service attacks against several major U.S. banks, including Bank of America, ING Bank and PNC Bank, and the U.S. Department of Justice also obtained the indictment of two Iranian men in 2018 in an international scheme that allegedly involved using malware to extort hospitals, public institutions and cities, including Atlanta.

"Iran has shown its cards in terms of their preferred targets, and they have a lot of resources and now they have the money, the people and the time to carry out such attacks," said Keith Frederick, chief information security officer at networking solutions provider RigNet. "It only takes one lucky strike to hit a home run."

While critical infrastructure is likely to be the primary target, experts stressed that no company would be off limits.

“Just because you don’t believe you have something of value to steal, that doesn’t mean you won’t be the target of a nation-state,” Mauriello said.

Given that bigger businesses typically have more mature cyber programs and defenses that are harder to crack, nation-state hackers could decide to seek out “low-hanging fruit” and exert less effort to hit a smaller company, where a disruption of service could still impact scores of Americans or could act as a gateway to a larger business, Mauriello added.

Social media could also prove to be an enticing avenue for sowing misinformation and unrest, according to Braun.

“People are highly dependent on social media, and it’s pretty clear that social media companies have

been too slow in dealing with this threat," Braun said.

Companies should also be on the lookout for an "increase in Iranian affiliated groups that are motivated by recent tensions but not acting at the tactical direction of the state," especially since these groups "have no incentive to be proportionate" in their strikes, according to John Carlin, a Morrison & Foerster LLP partner and former assistant attorney general for the DOJ's national security division.

In their efforts to evaluate whether their cybersecurity efforts are up to par, companies should look to the recent DHS bulletin, which encourages companies to employ "basic cyber hygiene practices, such as effecting data backups and employing multifactor authentication," and directs them to a link with more resources.

"If a company is adhering to best practices and doing it well, then it's likely to be way ahead of the curve and much better situated for not only preventing an attack, but being able to be in a position to much more effectively respond to an attack if it occurs," said Savage, the associate managing director at Kroll. "Nation-state threats are a whole other ballgame, so companies need to think about being prepared and make sure that as their business evolves, so are their cybersecurity practices and risk management practices."

The regulatory warnings also encourage companies to share any suspicious activity with the government, serving as a "force multiplier" to help more quickly identify novel threats, according to RigNet's Frederick.

And while political tensions with Iran may be subsiding for now, after President Donald Trump said Wednesday that the Islamic republic "appears to be standing down" and that the U.S. was "ready to embrace peace," Iran is widely expected to still be aggressive on the cyber warfare front, and companies need to continue to carefully monitor the lingering threat.

"The biggest thing to understand is that this threat is ongoing and it's real," Savage said.

--Editing by Philip Shea and Jill Coffey.