Why the Threat of an Iranian Cyberattack Should Matter to Your Organization

January 2020

The ongoing Iran-US tensions, and potential for retaliatory cyberattacks, call attention to the need for all organizations to consider whether they are prepared to defend against a cyberattack. Iran has a history of sophisticated cyberattacks in response to increased tensions, and we recommend a thorough review of your people, facilities, networks and data procedures in response to this increased threat environment.

The current Iran-US tensions follow a lethal US drone strike in Iraq that killed Iran's top military general, as well as an allied Iraqi military commander. In response, Iran's Supreme Leader Ayatollah Ali Khamenei warned that "harsh retaliation is waiting" and launched a series of missile attacks early January 8 (local time) against two Iraqi bases housing US troops, in Erbil and Al-Asad Air Base. While Javad Zarif, Foreign Minister of the Islamic Republic of Iran, tweeted after the attacks that, "[w]e do not seek escalation of war," it is unclear whether further retaliatory action will be taken by Iran directly or by its allies in the region.

Of all the tools Tehran has to retaliate, including its large military, Iranian-backed proxies around the Middle East and robust disinformation operations, international experts believe there is a strong likelihood that Iran will utilize its well-known cyber-warfare capabilities to inflict further damage over time. Both the US and the UK, a close ally in the Middle East, are on high alert to cyberattacks from Iran, which British intelligence agencies consider to be in the "Champions League" of cyber-warfare.

While there is no information indicating a specific, credible threat to the US or its allies, Iran and its partners have demonstrated the intent and ability to conduct operations in the US. It is widely believed that Iran first ramped up its cyberwar capabilities in response to a joint US-Israel cyber operation, which deployed the malware known as Stuxnet in the Natanz uranium enrichment facility in 2007, destroying centrifuges and crippling the country's nuclear efforts. Since then, Iran has repeatedly shown that it is a formidable cyber power with the tools to do real damage to government and private sector entities, including exfiltrating confidential, proprietary or sensitive personal data, shutting down websites or hijacking IT systems that run critical infrastructure and business functions.

Over the past decade, Iran has carried out cyberattacks on US organizations. Between 2010 and 2011, Iranian hackers launched a series of Distributed Denial of Services (DDoS) attacks that left hundreds of thousands of customers unable to access their financial accounts at JP Morgan, Bank of America and Capital One. In 2013, Iranian hackers took remote control access over a dam outside of New York, which, but for the gate being disconnected for maintenance, could have allowed the hackers to release water from the dam. Further, in 2014, Iranian hackers hit the Las Vegas Sands Corporation with a wiper malware, debilitating IT systems, knocking phone systems offline and rendering computers and servers unusable, after owner Sheldon Adelson suggested a nuclear strike against the country. In 2018, two Iranians were indicted by the Department of Justice for the SamSam ransomware attack that crippled Atlanta, costing the city millions to clean-up. Most recently, on January 5, 2020, the Federal Depository Library Program website was defaced by hackers claiming to work for the Iranian government. While there is no evidence linking this latest attack to Iran, it shows that the US government remains a target of pro-Iranian cyberattacks.

In response to this threat, on January 4, 2020, the Department of Homeland Security (DHS), issued a Bulletin, warning that, "Iran maintains a robust cyber program and can execute cyberattacks against the United States" and that, "[a]n attack in the homeland may come with little or no warning." Echoing the federal government's concern, the same day, New York's Department of Financial Services issued an Industry Letter warning that, "[t]here is currently a heightened risk of cyberattacks from hackers affiliated with the Iranian government," noting that, "Iran has a history of launching cyberattacks against the U.S., and the financial services industry." On January 6, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert stating that, "recent Iran-U.S. tensions have the potential for retaliatory aggression against the U.S." and that organizations should, "assess and strengthen [] cyber and physical defenses to protect against this potential threat."

What Does This Mean for Your Organization?

Iran and other state-sponsored cyber threat actors have seemingly endless resources and human capital, and can inflict significant damage from afar. To protect against this threat, organizations must take responsibility for implementing their own defense against cyber threats. Companies with a high profile or high symbolic value – particularly those perceived as being aligned with the US government or anti-Iranian activities – may become targets. Although your organization may not be the direct target of an Iranian cyberattack, it could be collateral damage, depending on the nature and scope of any retaliatory actions that may be forthcoming.

What Immediate Steps Can My Organization Take Today?

- Increase organizational vigilance and awareness, and update training and communications on phishing, internet risks and similar attack vectors.
- Instruct personnel to remain on guard for individuals soliciting information about your organization or its personnel.
- Deploy endpoint monitoring and multi-factor authentication as broadly as possible.
- Confirm reporting procedures in the event of a cyberattack and update related training and communications.
- Review your organization's Incident Response Plan (IRP), and carry out general and targeted training and communications on the plan.
- Make sure your organization's vulnerability management program and procedures, including security patches and penetration testing, are up to date.
- Make sure your organization's disaster recovery and business continuity program is in place and up to date.
- Confirm offline backups of critical information for operations.

What Should My Organization Consider Implementing Going Forward?

Develop or update your IRP – An IRP sets forth the key steps that organizations needs to immediately take during a cyber-incident. For example, an IRP will set forth reporting escalation procedures and alternative communication plans, and will create a response team of stakeholders and outside experts to assist with the response. Having a plan in place prior to an attack positions your organization to efficiently act in a measured, calm and unified manner.

Ensure your personnel are adequately trained – Given that a common method of attack is through email phishing or downloads from malicious websites, an effective defense mechanism is to train your personnel on the basics of cyber-hygiene. Likewise, your response team should conduct at least yearly exercises to practice its response in accordance with the IRP.

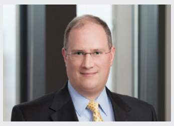
Understand where your data is located and what type of data you own – Regulators around the world have various laws on reporting obligations that are dependent upon the type of data compromised by a cyberattack. Likewise, the laws vary on the timing of the notification (e.g., 72-hours under the General Data Protection Regulation) and to whom the notification is made (e.g., regulators and/or data subjects). As such, mapping your data will guide your organization on its notification risks, obligations and the measures necessary to protect your data.

Conduct a Cybersecurity Risk Assessment (Assessment) – The purpose of an Assessment is to identify cybersecurity vulnerabilities in an organizations policies, procedures and IT environment, and to provide remediation strategies as appropriate. An Assessment conducted by an outside IT vendor that specializes in ethical hacking on behalf of an organization is an effective way to identify vulnerabilities in an organization. All Assessments should be conducted under the direction of counsel to ensure that the findings of the Assessment are protected by attorney-client privilege, the attorney work product or other applicable privileges. Should your organization become involved in litigation or other inquiry, protecting the Assessment, which sets forth in detail your cyber vulnerabilities, under privilege, is critical.

While your organization may not be the target of a pro-Iranian cyberattacks, there is no better time than now to ask and respond to this question: *Is my organization as secure as it can be and ready to respond if our defenses are breached*?

Contacts

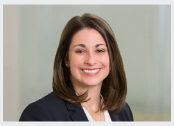
For more information on cybersecurity related topics such as the one discussed here, please contact one of the lawyers listed here.



Colin R. Jennings
Partner, Cleveland
T +1 216 479 8420
E colin.jennings@squirepb.com

Ann J. LaFrance
Partner, New York
T +1 212 872 9830
E ann.lafrance@squirepb.com

Garon Anthony
Partner, Birmingham
T +44 121 222 3507
E garon.anthony@squirepb.com



Ericka A. Johnson
Associate, Washington DC
T +1 202 457 6110
E ericka.johnson@squirepb.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations, nor should they be considered a substitute for taking legal advice.