THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 37 No. 3 March 2021

CYBER THREATS FROM NORTH KOREA AND CHINA: RISKS AND RECOMMENDATIONS

In April and May 2020, six different U.S. federal government agencies published two joint advisories regarding cyber threats from North Korea and China. Each advisory provides a summary of the potential risks and threats posed by each country to financial institutions and other sectors, best practices to guard against such risks, and associated legal requirements. The authors discuss these advisories, the practical implications for the private sector, and the U.S. government's expectations for compliance.

By Mario Mancuso, Sanjay Mullick, and Jeremy Iloulian *

In the last few years, the United States has imposed increasingly severe restrictions on North Korea and China, such as economic sanctions and export controls, in the interests of U.S. foreign policy and national security priorities. Given U.S. market power, these restrictions have placed a strain on North Korea's efforts to acquire money and other resources, and China's efforts to acquire advanced technologies. Whether as a reason for, or in response to, these U.S. policies, cyberattacks serve as a flashpoint for tensions with North Korea and China, and provide a theater of conflict where they can pose an asymmetric threat not only to the United States government, but also to the private sector.

I. WHAT IS SYSTEMIC RISK?

The U.S. government recently issued two cyber threat advisories, one discussing threats from North Korea and one discussing threats from China, with both indicating that public and private sector institutions in the U.S. are at risk of cyberattacks (collectively, the "Advisories"). Both also acknowledge that these attacks are either directly attributable to North Korea or China, or stem from organizations or persons that act at the direction of either country.

A. North Korea

On April 15, 2020, the Department of State, Department of the Treasury, Department of Homeland Security, and Federal Bureau of Investigation issued a comprehensive joint advisory on the risks of a North Korean cyber threat (the "DPRK Cyber Threat Advisory").[1] The DPRK Cyber Threat Advisory

[1] DPRK Cyber Threat Advisory: Guidance on the North Korean Cyber Threat (Apr. 15, 2020), https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf.

* *MARIO MANCUSO is a partner and leads the International Trade and National Security practice in the Washington, D.C. office of Kirkland & Ellis LLP. SANJAY MULLICK is a partner and JEREMY ILOULIAN is an associate in the same practice. Their e-mail addresses are mario.mancuso@kirkland.com, sanjay.mullick@kirkland.com, and jeremy.iloulian@kirkland.com. ANJULI DAS also contributed to this article.*

RSCR Publications LLC Published 12 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $650 per year in U.S., Canada, and Mexico; $695 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 1051-1741.

underscores the depth and breadth of North Korea's malicious cyber activities, stating:

> The DPRK has the capability to conduct disruptive or destructive cyber activities affecting U.S. critical infrastructure. The DPRK also uses cyber capabilities to steal from financial institutions, and has demonstrated a pattern of disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible State behavior in cyberspace.[2]

The DPRK's cyberattacks stem from its inability to receive financing because U.S. and United Nations sanctions have isolated North Korea from international commerce and from the global banking system. Without access to commercial relationships or global financial institutions, its financial situation has been precarious at best and its economy devastated at worst.

These sanctions include an embargo that prohibits all U.S. persons, regardless of whether such persons are physically within the United States, from engaging in any dealings (*e.g.*, exports, imports, investments) with any individuals or entities that are located in, organized under the laws of, or otherwise nationals of North Korea.[3] Moreover, the Treasury's Office of Foreign Assets Control ("OFAC") has an extensive list of individuals, entities, and even vessels designated on U.S. sanctions lists, often those affiliated with the North Korea government, military, or leadership, with whom U.S. persons also cannot transact.[4] Even without a U.S. person, such transactions may be prohibited if they involve U.S. dollars or U.S.-origin goods, software, or technology.

North Korea's own behavior is what has resulted in sanctions, including condemnation from the international community in the form of UN sanctions. However, North Korea's marginalization from the conventional channels of trade and finance has led it to use cyberattacks to try to evade sanctions and gain access to financial resources. The DPRK Cyber Threat Advisory focuses on identifying the industries that may be potential targets, the types of attacks, and the best practices companies can take to reduce their risk of such an attack.

B. China

Relatedly, on May 13, 2020, the FBI along with the Cybersecurity and Infrastructure Security Agency ("CISA"), a branch of DHS, issued a shorter separate public service announcement discussing China's cyber targeting of research organizations ("China Cyber Threat PSA").[5] The China Cyber Threat PSA focuses on the desire of cyber actors affiliated with China to use cyberattacks to obtain research and development associated with COVID-19, stating:

> These actors have been observed attempting to identify and illicitly obtain valuable intellectual property ("IP") and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research. The potential theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options.[6]

The China Cyber Threat PSA also provides recommendations for cybersecurity practices to "prevent surreptitious review or theft of COVID-19 material."[7]

---

[2] *Id.* at 1.

[3] 31 C.F.R. § 510.

[4] The property of any party on a sanctions-restricted party list is subject to "blocking" should it come within the possession or control of a U.S. person or come within the jurisdiction of the United States. This means the U.S. person must notify OFAC of its possession and may not take any further action with respect to the property without OFAC's approval.

[5] U.S. Federal Bureau of Investigation and Cybersecurity Infrastructure and Security Agency, Public Service Announcement: People's Republic of China ("PRC") Targeting of COVID-19 Research Organizations (May 13, 2020), https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.

[6] *Id.*

[7] *Id.*

The China Cyber Threat PSA reflects the view that the United States and China are engaged in a "strategic competition" to assert leadership over advanced technologies, and a growing belief in the United States that China is willing to acquire them by "unfair" means. The Trump administration's December 2017 National Security Strategy crystallized its concerns in this area, stating, *e.g.*, that "competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars."[8]

Part of the concern is that China's Made in China 2025 and China Standards 2035 programs, both initiatives where the Chinese government directs significant funding to develop certain advanced technologies, also include systematic efforts by the Chinese government to acquire select U.S. technology companies or to engage in cyber espionage.[9] The "trade war," which resulted in the United States imposing tariffs on $370 billion of imports from China, was triggered in part by the underlying belief that "China conducts and supports unauthorized intrusions into, and theft from, the computer networks of U.S. companies to access their sensitive commercial information and trade secrets," and China strategically acquires advanced technology companies.[10]

To counter Chinese acquisition of and access to American technology, the U.S. responded by upgrading regulations for reviewing proposed investments in the United States through the Committee on Foreign Investment in the United States ("CFIUS") and modernizing its export control rules to include "emerging and foundational technologies."[11] Furthermore, a number of Chinese technology companies, such as Huawei, have been designated on U.S. export-restricted party lists in order to deny them access to U.S. dual-use technology needed for initiatives such as 5G communications.[12]

Alerting the public through the China Cyber Security PSA and other similar mechanisms is just another action the U.S. government is taking in its strategic competition with China. This takes on heightened significance because the China Cyber Security PSA focuses on COVID-19 responses, a subject on which Washington and Beijing have traded barbs, including as to whether China was sufficiently and promptly transparent about the seriousness and spread of COVID-19. This raises the stakes of both stealing and safeguarding corresponding intellectual property and relevant public health data.

II. EXAMPLES OF CYBER THREATS

The root causes of North Korea's and China's actions highlight the cybersecurity threats that each country poses to the United States, other countries, and the private sector. The Advisories describe each of these threats and the industries affected, with the DPRK Cyber Threat Advisory expounding on the threats in detail. However, though only the DPRK Cyber Threat Advisory provides examples of such attacks, there are numerous apparent examples of China engaging in similar behavior.

A. North Korea

The DPRK Cyber Threat Advisory examines three specific cyber threats that private industry faces: cryptojacking, financial theft and money laundering, and extortion. The DPRK Cyber Threat Advisory cites to information provided by the United Nations Security Council 1718 Committee Panel of Experts ("UNSC 1718 Committee") 2019 mid-term report ("2019 UNSC Report") about North Korea's suspected activities.[13]

[8] EXEC. OFFICE OF THE PRESIDENT, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA (Dec. 2017).

[9] *Id.*

[10] Notice of Determination and Request for Public Comment, 67 Fed. Reg. 14,907 (Apr. 6, 2018) ("China directs and unfairly facilitates the systematic investment in, and acquisition of, U.S. companies and assets by Chinese companies to obtain cutting-edge technologies and intellectual property, and generate the transfer of technology to Chinese companies.").

[11] Foreign Investment Risk Review Modernization Act, 31 C.F.R. § 801 (Jan. 13, 2020); Export Control Reform Act, 50 U.S.C. 58 (2018).

[12] Addition of Entities to the Entity List, 15 C.F.R. § 744 (May 21, 2019); Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, 15 C.F.R. § 744 (Aug. 21, 2019); Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, 15 C.F.R. § 730, 732, 736,744 (May 19, 2020).

[13] UNSC 1718 Committee Panel of Experts, S/2019/691 (Aug. 30, 2019), https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.

1. Cryptojacking.

Cryptojacking is a method of cryptomining that uses a malware mechanism to infiltrate a computer, infecting its systems, and causing it to mine digital currency surreptitiously. The UNSC 1718 Committee documented several instances where compromised computers sent mined digital currency to North Korea, identified as the destination by the location of the servers. In some instances, the servers were located at Kim Il Sung University. Often the assets the computers mined were anonymity-enhanced digital currency, also known as "privacy coins," making them harder to track since neither the sender nor the receiver of privacy coins can be digitally identified.

This type of attack can happen to any entity with computing resources, regardless of location, and it highlights North Korea's efforts to acquire additional financial resources in the face of overwhelming economic sanctions. The UNSC 1718 Committee is still investigating these incidents for potential UN sanctions violations.

2. Digital Currency Money Laundering and the FASTCash Financial Theft.

As with cryptojacking, there are numerous identified instances of North Korea attempting to acquire financial resources by stealing from major financial institutions. The 2019 UNSC Report notes that North Korea has attempted dozens of times to steal up to $2 billion by means of cyber theft. North Korean actors have hacked into digital currency exchanges and stolen the equivalent of hundreds of millions of dollars in digital currency. A recent DOJ forfeiture complaint identified similar actions, noting that the actors involved used North Korean infrastructure to engage in these activities.[14] After stealing these financial resources, the North Korean actors laundered the funds through legitimate channels, such as non-North Korean financial institutions, in order to collect the currency.

For example, in February 2016, DPRK state-sponsored cyber actors apparently attempted to steal $1 billion from a series of financial institutions and succeeded in stealing $81 million from the Bangladesh Bank by sending spear phishing e-mails (messages that appear to be from trusted senders, thereby deceiving recipients into revealing confidential information) to bank employees. With this information, DPRK state-sponsored cyber actors were able to access the bank's computer terminals, which interfaced with the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") network. The conspirators then sent fraudulent messages over SWIFT to the Federal Reserve Bank of New York, authorizing a transfer of funds from the Bangladesh Bank's account to their own.[15]

Similarly, in April 2018, DPRK state-sponsored cyber actors stole almost $250 million in digital currency from a digital currency exchange after hacking it. The cyber actors then laundered the money through hundreds of automated exchanges, with the alleged assistance of two Chinese nationals, in an attempt to prevent its origins from being tracked by authorities.[16]

The emergence of FASTCash schemes over a period of several years provides another example of DPRK state-sponsored hacking. FASTCash schemes, which first emerged in 2016, compromise banks' payment switch application servers so that cyber actors can remotely trigger cash withdrawal from a large number of ATMs simultaneously. Multiple DPRK state-sponsored FASTCash schemes in 2017 and 2018 enabled simultaneous cash withdrawal from ATMs across 20 to 30 countries each.[17]

Due to comprehensive U.S. sanctions, as well the Financial Action Task Force's ("FATF") designation of North Korea as a "High Risk Jurisdiction" with respect to money laundering, North Korean financial institutions effectively have been ostracized from the global financial system.[18] North Korea's cyber threats have supported its efforts to try to work around these prohibitions.

3. Cyber Extortion.

Cyber extortion is similar to other types of efforts to extort others in order to obtain a ransom. According to a separate OFAC advisory on how U.S. persons should respond to ransomware, such cases have been increasing, with a 37% increase in reported cases and a 147% increase in associated losses from 2018 to 2019.[19]

[14] DPRK Cyber Threat Advisory, *supra* note 1.

[15] DPRK Cyber Threat Advisory, *supra* note 1.

[16] *Id.*

[17] *Id.*

[18] FINANCIAL ACTION TASK FORCE, *High-Risk and Other Monitored Jurisdictions*, http://www.fatf-gafi.org/countries/#high-risk (last visited June 17, 2020).

[19] U.S. Department of the Treasury Office of Foreign Assets Control, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020)

In this case, North Korean actors use cyber tools to compromise an entire network. After doing so, they threaten to shut down the network unless paid a ransom. Ironically, North Korean cyber actors at times gain access to these networks by promoting themselves as consultants who can help prevent future malicious cyberattacks. Sometimes these actors will offer their services to extort a third party, such as by hacking the website of a rival private entity or organization.

Outside of the financial sector, since 2017, North Korea has been willing to target healthcare, education, and other sectors, and demand ransom through the use of "WannaCry 2.0."[20] This is ransomware, developed by DPRK state-sponsored cyber actors and Chinese nationals, that encrypts an infected computer's data. The cyber actors can then demand payment of a ransom in bitcoin digital currency in return for unencrypting the hijacked data. The WannaCry 2.0 ransomware attacks became so prevalent that each of the Five Eyes countries (the United States and four countries with significant intelligence sharing networks – Australia, Canada, New Zealand, and the United Kingdom), as well as Denmark and Japan – issued statements attributing the attacks to North Korea.

Perhaps surprisingly, even Hollywood has been a target, as seen in the attack on Sony Pictures from DPRK state-sponsored cyber actors. The cyber actors stole confidential information, damaged thousands of computers, and threatened staff in response to Sony Pictures producing the film "The Interview," which mocked North Korea's leader, Kim Jong-un. The OFAC Ransomware Advisory provides further guidance, noting that ransomware attacks, even if not from North Korea, target a variety of entities, including small- and medium-sized businesses, local governments, school districts, and hospitals.

B. China

Unlike the DPRK Cyber Threat Advisory, the China Cyber Threat PSA does not cite specific historical examples, but it still notes the risk to companies "that play a critical role in COVID-19 research and response."[21] The China Cyber Threat PSA specifically identifies those companies involved with vaccines, treatments, and testing from networks and personnel affiliated with COVID-19 research.

Although the China Cyber Threat PSA is focused on organizations involved in the COVID-19 response, there are also numerous examples from the last few years of Chinese cyberattacks against private industry, believed to have occurred at the direction of the Chinese government. Some of the industries targeted include defense and aerospace, utilities, banking, construction, manufacturing, telecommunications, and media.[22]

The China Cyber Threat PSA identifies the two primary items of interest for Chinese cyber actors as intellectual property and public health data.

1. Using Hacking, Malware, and Researchers to Steal Intellectual Property.

In late July 2020 a federal grand jury in Spokane, Washington, indicted Chinese nationals Li Xiaoyu and Dong Jiazhi for hacking into hundreds of computer systems belonging to a wide range of individuals, governments, and organizations both for personal financial gain and on behalf of the Chinese Ministry of State Security ("MSS"), a Chinese government agency.[23] The indictment alleges the hacking campaign lasted more than 10 years and targeted high-tech manufacturing, engineering, software, defense, and pharmaceutical industries in at least 13 countries. Its most recent targets included organizations researching COVID-19, including potential vaccines, testing, technology, and treatments. The 11-count indictment notes that these attacks had neither any particular geographic limits, as targets were located throughout Europe, the United States, and the Asia-Pacific region, nor any limits on the types of targets, which included

footnote continued from previous page…

https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[20] DPRK Cyber Threat Advisory, *supra* note 1.

[21] China Cyber Threat PSA, *supra* note 5.

[22] U.S. Federal Bureau of Investigation, China Case Example: Chinese Cyber Hackers' Targeting of U.S. Aerospace and Military Intellectual Property (2019), https://www.fbi.gov/file-repository/china-case-example-aerospace-military-2019.pdf/view; Maggie Miller, *Experts report recent increase in Chinese group's cyberattacks*, THE HILL (Mar. 25, 2020), https://thehill.com/policy/cybersecurity/489531-experts-discover-recent-increase-in-chinese-cyberattacks.

[23] Press Release, U.S. Department of Justice, Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research (July 21, 2020), https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

governments, non-governmental organizations, clergy, dissidents, and democracy and human rights activists.

Recently, a concern for the U.S. government, based on a separate July 2020 FBI alert from its cyber division, is a malware from China called "Goldenspy." Once installed, Goldenspy provides a backdoor into a company's system.[24] The malware is often included in installations that Chinese banks may require of foreign parties to engage in transactions. The malware has been installed on company systems since 2016, making it difficult for the U.S. government to determine how many companies have potentially been infected. Like the China Cyber Threat PSA, the July 2020 alert notes that the likely targets include the healthcare sector, specifically pharmaceutical companies, but also notes that the chemical and financial sectors are equally vulnerable.

A similar example to the two above, dating from before COVID-19's spread, was the December 2018 DOJ indictment of two Chinese nationals, Zhu Hua and Zhang Shilong, also allegedly tied to the MSS. The indictment alleges that the two nationals worked with a Chinese company that acted in coordination with the MSS and engaged in cyberattacks to steal intellectual property and confidential business information, predominately from technology companies. These attacks occurred over a 12-year period and involved over 45 companies in at least 12 U.S. states.[25]

Though intellectual property theft in many instances is related to a cyber breach, some well-known instances of IP theft in the medical field stem from persons who sought to transfer material or knowledge from one location to another. In one example from September 2019, the DOJ charged a couple – Yu Zhou and Li Chen – who worked for Nationwide Children's Hospital's Research Institute in San Diego, with stealing scientific trade secrets related to medical research from the hospital.[26] The couple founded a company in China in 2015 without the hospital's knowledge and, through the company, provided research and related services using the hospital's research and left the hospital after receiving payment for such work. Here, the parties involved were close to the hospital itself, demonstrating the need for a more rigorous compliance system.

While this is a more brazen example, it shows that intellectual property theft may not be limited strictly to designs or a computer code. It also reflects a growing concern in Congress about researchers in the United States taking their research to China, specifically via China's Thousand Talents Program, which attempts to recruit top scientists to China.[27]

These examples provide a sense of the priorities of Chinese cyber actors and of the lengths to which they will go to acquire intellectual property. Given the types of intellectual property at stake (*e.g.*, COVID-19 vaccines), companies should consider what such actors are willing to do when provided with sophisticated cyber tools.

2. Cyberattacks to Breach Public Health Data.

One instance of a comparable cyberattack focusing on public health data is a series of data breaches of Anthem Inc., a major private health insurance company, which the DOJ alleged Chinese actors conducted from February 2014 to January 2015.[28] According to the DOJ, these actors stole from Anthem's servers personally identifiable information ("PII") of over 78 million people. These major data breaches could be an indicator of the targets of future cyberattacks.

---

[24] U.S. Federal Bureau of Investigation, Cyber Division, Chinese Government-Mandated Tax Software Contains Malware, Enabling Backdoor Access (July 23, 2020) [hereinafter July 2020 FBI Alert], https://www.ic3.gov/media/news/2020/200728.pdf.

[25] Press Release, U.S. Department of Justice, Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information (Dec. 20, 2018), https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[26] Press Release, U.S. Department of Justice, Couple Who Worked at Local Research Institute for 10 Years Charged with Stealing Trade Secrets, Wire Fraud (Sept. 16, 2019), https://www.justice.gov/opa/pr/couple-who-worked-local-research-institute-10-years-charged-stealing-trade-secrets-wire-fraud.

[27] Mark Magnier, *FBI and US Senate raise alarm over China's recruitment of US scientists*, THE SOUTH CHINA MORNING POST, Nov. 20, 2019, https://www.scmp.com/news/china/politics/article/3038491/fbi-and-us-senate-raise-alarm-over-chinas-recruitment-us.

[28] Press Release, U.S. Department of Justice, Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People (May 9, 2019).

Attacks seeking public health data can also extend outside the public health sector. For example, credit-reporting agency Equifax was targeted due to the massive amount of PII it holds. A recent DOJ indictment for this case alleged that, in 2017, four members of China's People's Liberation Army engaged in a months-long effort to steal the PII of almost 150 million Americans.[29]

Recent cyberattacks also extend beyond U.S. companies. For example, in January 2020, Mitsubishi Electric Corp. claimed it was the target of an "extensive" cyberattack from Chinese hackers targeting information regarding business partners and government sources.[30] Mitsubishi claimed no information was compromised, but the attack itself shows that a wide variety of companies could be potential targets.

III. ACTION ITEMS FOR INDUSTRY

The Advisories prescribe a series of measures that companies can take to safeguard against these cyberattacks, as well as actions to take in the event of a cyberattack. These can be broken into four major groupings: implement cybersecurity best practices; adopt U.S. government cybersecurity guidance; strengthen anti-money laundering compliance systems; and cooperate with law enforcement.

A. Implement Cybersecurity Best Practices

The DPRK Cyber Threat Advisory identifies a number of best practices that companies can enact to try to prevent or thwart an attack or to reduce its impact. It also highlights the importance of implementing these measures, especially for financial institutions. The measures named include: (1) segmenting networks to limit the amount of data that can be accessed in any particular one; (2) making backup copies of data to provide redundancy; (3) conducting training to identify social engineering tactics, including information-sharing and network access policies; and (4) implementing cyberattack response strategies.

The China Cyber Threat Advisory further recommends companies patch all systems for critical vulnerabilities. It notes that priority should be given to internet-connected servers and software processing internet data, as those are more vulnerable to cyberattack from outside actors than networks that are private or local. Companies should also actively scan their servers and applications for potential unauthorized access, modification, or anomalous activities, as those could be indicators of attempts to penetrate the network. It recommends as a best practice imposing more stringent requirements for logging into systems, such as multi-factor authentication, as this can better prevent access by illegitimate users.

Further, subsequent FBI alerts have recommended that systems establish a baseline for what is standard network activity to better identify unusual activity and to suspend access by individuals associated with such activity.[31] This is in addition to segmenting critical information on "air-gapped systems" (systems without any network interfaces to other networks) and implementing stricter controls for persons to access critical data. Given the GoldenSpy malware, there is also a recommendation for companies to scrutinize any joint ventures, particularly involving biosciences, that involve cyber infrastructure, new or otherwise.

B. Adopt U.S. Government Cybersecurity Guidance

A number of agencies have provided guidance for industry to use in developing these types of policies and procedures, such as the National Institute of Standards and Technology ("NIST") Cybersecurity Framework. The NIST Cybersecurity Framework itself recognizes the complexity of these challenges, noting:

> Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework.[32]

The DPRK Cyber Threat Advisory also references the Department of Energy's Cybersecurity Capability Maturity Model ("DOE C2M2") as a program worth reviewing. The DOE C2M2 is a public-private partnership specifically to enhance the cybersecurity of power grids and other energy-related entities.[33] The

[29] Press Release, U.S. Department of Justice, Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax (Feb. 10, 2020).

[30] Julian Ryall, *Japan's Mitsubishi Electric targeted in cyberattack blamed on Chinese hackers*, THE SOUTH CHINA MORNING POST, Jan. 20, 2020, https://www.scmp.com/week-asia/economics/article/3046825/japans-mitsubishi-electric-targeted-cyberattack-blamed-Chinese.

[31] July 2020 FBI Alert, *supra* note 24.

[32] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Apr. 16, 2018).

[33] OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, U.S. DEPARTMENT OF ENERGY, CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) PROGRAM, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-

DOE C2M2 is publicly available and the DOE has provided variations depending on the requesting entity (*e.g.*, oil and gas companies, electricity companies).

Finally, CISA itself, as a subset of DHS, is one of the primary federal agencies to protect critical infrastructure from cyberattacks, and in turn has a host of materials available for guidance. The DPRK Cyber Threat Advisory conveniently lists these materials in its Annex I.

One example is CISA's "STOP. THINK. CONNECT" campaign, which is meant to inform the public about cybersecurity risks and compliance measures.[34] CISA published a toolkit associated with this campaign that includes 20 different tip sheets and advisories depending on the industry or the activity involved, from mobile banking to online gaming.[35] Moreover, CISA offers training and cybersecurity exercises to help private entities prevent potential attacks, identify any attacks, and respond when there is a breach.[36]

C. Strengthen Anti-Money Laundering Compliance

Anti-money laundering laws often apply to all companies within the relevant jurisdiction, but the more stringent requirements are for those considered financial institutions or similar types of businesses. The DPRK Cyber Threat Advisory reminds U.S. financial institutions and other covered businesses and persons to comply with the Bank Secrecy Act, the primary anti-money laundering statute implemented by the Treasury's Financial Crimes Enforcement Network ("FinCEN"). Importantly, "developing and maintaining effective anti-money laundering programs . . . as well as identifying and reporting suspicious transactions" are core requirements for financial institutions.[37]

Though non-U.S. financial institutions already should comply with all applicable laws, the DPRK Cyber Threat Advisory makes clear that the United States is pushing for other countries to adopt international standards as described by FATF as well. Part of this effort involves getting other countries to pressure non-U.S. financial institutions to pay particular attention to transactions involving North Korea, similar to how the U.S. has advocated for other countries to adopt economic sanctions.

For digital asset service providers, the DPRK Cyber Threat Advisory highlights the importance of remaining alert to changes in customers' activities. It indicates these institutions have a higher risk of being used for money laundering, financing terror, and weapons of mass destruction financing. The digital asset service providers of greater concern are those with anonymous payment accounts or suspicious reporting and customer diligence.

D. Cooperate with Law Enforcement

The DPRK Cyber Threat Advisory highlights the importance of companies notifying law enforcement agencies as expeditiously as possible if they suspect a cyberattack. The sooner a private party notifies law enforcement, the higher the chance any stolen assets can be recovered. The China Cyber Threat Advisory notes that, to report any suspicious or criminal activity, a target or victim of a cyberattack should contact the local FBI field office.

In their review of such cyberattacks, U.S. authorities have seized millions of dollars' worth of assets, primarily digital currency, stolen by cyber actors with ties to North Korea. Additionally, OFAC has a sanctions program related to significant malicious cyber-enabled activities, which could be applied to Chinese and North Korean parties, among others.[38] This program authorizes OFAC to identify bad actors as having engaged in certain cyber activities and designate them on a restricted party list subject to blocking. Providing information to the applicable government agencies can lead to the appropriate parties being subject to U.S. sanctions.

footnote continued from previous page…

cybersecurity-0#:~:text=The%20Cybersecurity%20Capability%20Maturity%20Model%20(C2M2)%20program%20is%20a%20public,cybersecurity%20posture%20of%20the%20grid.

[34] *STOP. THINK. CONNECT.*™, U.S. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (last revised Jan. 7, 2020), https://www.cisa.gov/stopthinkconnect.

[35] *STOP. THINK. CONNECT.*™ *Toolkit,* U.S. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (last revised Aug. 6, 2020), https://www.cisa.gov/publication/stop-think-connect-toolkit.

[36] *Cybersecurity Training and Exercises*, U.S. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (last revised July 15, 2020), https://www.cisa.gov/cybersecurity-training-exercises.

[37] DPRK Cyber Threat Advisory, *supra* note 1.

[38] 31 C.F.R. § 578.

It is possible that in the course of the applicable law enforcement's investigation, the investigators will contact financial institutions for information. The DPRK Cyber Threat Advisory makes clear that cooperating with U.S. law enforcement on these investigations is critical, particularly to support the seizure of stolen assets. In some instances, the U.S. government provides financial rewards of up to $5 million for providing information about DPRK cyber activities through the Rewards for Justice program.[39]

IV. MEETING U.S. GOVERNMENT COMPLIANCE EXPECTATIONS

Both cyberattacks and sanctions are set against an important compliance backdrop that the U.S. government considers a high priority. The North Korean and Chinese actors engaging in breaches and other behavior would be the ultimate focus of penalties and other consequences. However, without adequate compliance measures in place, U.S. companies and U.S. financial institutions that are targets or commit violations inadvertently may not be eligible for mitigation from the U.S. government and could be penalized as well. Even non-U.S. companies and non-U.S. financial institutions need to pay attention.

A. The Advisories

The best practices described in the Advisories are measures that the U.S. government has advised private industry to strive to implement. Without these measures, the government may be limited in its ability to assist a company that has suffered a cyberattack, *e.g.*, to successfully track down stolen assets. The government may also be less sympathetic to an entity that has suffered a cyberattack, but that did not implement recommended mechanisms to mitigate against one.

The risk of such a negative feedback loop is accentuated by the fact that some of the best practices actually stem from legal requirements that already exist, such as compliance with required NIST cybersecurity standards for government contractors.[40] For example, if a company were under an independent obligation to timely disclose to the U.S. government that it had suffered a cyberattack, in doing so the company might also reveal to the government that it had breached its legal obligations by not having required compliance safeguards in place.

With respect to China, in today's environment, this could be particularly crucial where companies are targets of Chinese cyber threats related to COVID-19, given the public health urgency and high stakes of achieving and safeguarding medical advances. Failure to have compliance safeguards could result in the U.S. government filing a claim for damages on the basis of either a breach of contract or the False Claims Act.

Another example is anti-money laundering standards. Financial institutions already are required to have in place compliance measures to combat against money laundering, such as Know Your Customer requirements, and they are under an obligation to report suspected activity. If a cyberattack occurred and the institution had not done so, the U.S. government could fine the institution up to $500,000, or double the amount of money that was laundered, whichever was greater, and/or company employees could face up to 20 years imprisonment.[41]

B. U.S. Sanctions

With respect to North Korea in particular, the core issue is that it is subject to comprehensive U.S. economic sanctions, a point affirmed in the DPRK Cyber Threat Advisory. As previously discussed, this means U.S. persons can have almost no interaction with North Korea or North Korean persons. Each violation of these economic sanctions potentially can result in civil penalties of either the greater of $307,922 or twice the value of the transaction,[42] or criminal penalties of up to $1,000,000 and/or 20 years imprisonment per violation.[43]

Importantly, economic sanctions are a strict liability regime. This means parties can be penalized for violations even if they were inadvertent, *e.g.*, if they did not know they were dealing with North Korea or a North Korean party. This challenge is magnified with respect to cyber actors, where such actors may specialize in disguising their true identities, *e.g.*, posing as cybersecurity specialists when they are actually cyber hackers connected to the North Korean government.

---

[39] Rewards for Justice, U.S. DEPARTMENT OF STATE, https://rewardsforjustice.net/english/.

[40] *See, e.g.*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS (Feb. 2020).

[41] 18 U.S.C. § 1956(a).

[42] 31 C.F.R. § 501, App. A (2019).

[43] *Id.*

Often, what determines whether violations of economic sanctions will result in higher penalties is whether OFAC determines that the conduct was "egregious," *e.g.*, that the party should have known it was a violation.[44] OFAC follows a series of factors to determine what constitutes an egregious violation, but now an important one is whether the party has a sanctions compliance program. In May 2019, OFAC issued a "Framework for Compliance Commitments," recommending that companies implement an effective Sanctions Compliance Program, consisting of at least five elements: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.[45]

The Framework puts the private sector on notice of what constitutes an effective compliance program and what OFAC might consider as a mitigating factor when assessing any potential violations. Having a compliance program that satisfies OFAC's expectations not only adds actual protection against a sanctions violation, but also can serve as a form of insurance policy in case of an inadvertent violation, to demonstrate to OFAC that the implementing company undertook recommended efforts to reduce risk. OFAC itself has indicated, *e.g.*, that it "will consider favorably subject persons that had effective SCPs at the time of an apparent violation," and may "consider the existence of an effective SCP at the time of an apparent violation as a factor in its analysis as to whether a case is deemed 'egregious'."[46]

In addition to the Framework, the OFAC Ransomware Advisory contemplates the possibility that the person demanding the ransomware payment may be in North Korea or on the OFAC List of Specially Designated Nationals and Blocked Persons ("SDN List"), with whom U.S. persons are prohibited from dealing.[47] A payment to the North Korean party in this instance, or facilitating such a payment (for financial institutions), would be considered a violation of U.S. sanctions. However, the OFAC Ransomware Advisory states that OFAC will consider any "self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome," indicating OFAC's preference for victims of ransomware attacks to communicate to the appropriate authorities. For financial institutions subject to more stringent anti-money laundering laws, there may be additional requirements with respect to FinCEN.[48]

C. Global Application and Implementation

Though U.S. sanctions apply to those subject to U.S. jurisdiction, such as U.S. persons, increasingly the United States has extended them extraterritorially to non-U.S. persons, implementing what is termed "secondary sanctions." With respect to North Korea, the primary authorities related to these secondary sanctions are the Korean Interdiction and Modernization of Sanctions Act ("KIMSA") within the Countering America's Adversaries Through Sanctions Act ("CAATSA") that entered into force in July 2017, and Executive Order 13810 from September 2017.[49]

Though secondary sanctions of course apply directly to their targets, they also have the important effect of deterring others from dealing with those targets. For example, under CAATSA and KIMSA, the United States can impose sanctions on non-U.S. parties that knowingly conducted or facilitated a "significant transaction" with or on behalf of North Korean sanctioned parties. The DPRK Cyber Threat Advisory provides that OFAC has the authority to impose sanctions on "[i]ndividuals and entities engaged in or supporting DPRK cyber-related activity," including those:

- engaged in significant activities undermining cybersecurity on behalf of the Government of North Korea or the Worker's Party of Korea;
- operating in the information technology industry in North Korea;
- engaged in certain other malicious cyber-enabled activities; or

[44] *Id.*

[45] U.S. DEPARTMENT OF THE TREASURY'S OFFICE OF FOREIGN ASSETS CONTROL, A FRAMEWORK FOR OFAC COMPLIANCE COMMITMENTS (May 2019). https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.

[46] *Id.*

[47] OFAC Ransomware Advisory, *supra* note 19.

[48] U.S. Department of the Treasury Financial Crimes Enforcement Network, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (Oct. 1, 2020), *supra* note 19.

[49] *See generally*, Countering America's Adversaries through Sanctions Act, 22 U.S.C. 9401 (2017); Korean Interdiction and Modernization of Sanctions Act 22 U.S.C. 9201 (2016); Exec. Order No. 13810; 31 C.F.R. § 510.201 (Sept. 25, 2017).

- engaged in at least one significant importation from or exportation to North Korea of any goods, services, or technology.[50]

Non-U.S. parties thus may adhere to U.S. restrictions in order to protect their own U.S. interests, such as their access to the U.S. market. This is a particularly acute concern for financial institutions processing financial transactions, as the DPRK Cyber Threat Advisory provides that, if an institution violates U.S. sanctions, "that institution may, among other potential restrictions, lose the ability to maintain a correspondent or payable-through account in the United States."[51] The status of the U.S. dollar as the world's reserve currency and the need to maintain access to the U.S. financial system are key considerations for non-U.S. companies and non-U.S. financial institutions in deciding to follow U.S. sanctions even in the absence of jurisdiction.

China is also increasingly exposed to U.S. secondary sanctions, both due to its shared border and close economic relationship with North Korea, as well as for its own reasons. For example, OFAC designated Dalian Global Unity Shipping Co., Ltd., a Chinese company involved in shipping resources and luxury goods to North Korea, on its SDN List. This prohibits Dalian from engaging in any transactions with U.S. persons or the U.S. financial system, even though Dalian has no apparent operations in the United States.[52]

Though U.S. economic sanctions are extensive and even extraterritorial, they are not global. For example, because the sanctions are stifling North Korea's access to resources, North Korean actors may be motivated and even forced to search for other jurisdictions that do not implement the same stringent standards as the United States and try to take advantage of those gaps in order to acquire financial resources. For cyber actors, this is a high-technology version of sanctions circumvention.

To try to close these gaps, beyond the force of law, the Advisories provide guidance for foreign governments. For example, the DPRK Cyber Threat Advisory provides guidance on information-sharing among governments and the private sector and on implementing international standards, such as UN sanctions or FATF guidelines. The United States is also engaging in efforts at a diplomatic level to encourage other countries to implement these changes. Depending on the success of these efforts, down the road one could see more strict rules in countries around the world as well.

V. CONCLUSION

The growth in the importance of online banking, advanced technologies, and big data for the private sector runs parallel to the increase in risks of cyberattacks to infiltrate and steal such resources. As the U.S. works to carry out various foreign policy and national security priorities, the private sector is also impacted, both directly by government restrictions, and indirectly through the response of foreign governments or state-owned entities targeting American industry. The United States is aware of both direct and indirect impacts, and is now communicating to the private sector the risks, legal obligations, and expectations, including through the publication of these Advisories.

In turn, the private sector should ensure the Advisories and the information within them are reviewed closely by compliance counsel, keeping in mind the larger context of some of the key foreign policy issues with which the United States is engaging. Private sector decision-makers should take the necessary steps or updates needed to meet the growing cyber threats from North Korea and China that the U.S. government has identified. Its corresponding recommendations for compliance further intertwine U.S. national security and regulatory requirements, increasing their significance beyond standard compliance best practices. ■

[50] DPRK Cyber Threat Advisory, *supra* note 1.

[51] *Id.*

[52] Press Release, U.S. Department of the Treasury, Treasury Acts to Increase Economic Pressure on North Korea and Protect the U.S. Financial System (June 29, 2017).