MOFOCUS

OUR INSIGHTS INTO THE RISK + CRISIS LANDSCAPE

Volume 1, Issue 1
2017

IN THIS ISSUE

EDITORS

John Carlin
Partner
New York/Washington, D.C.

David Newman
Of Counsel
New York

Sophia Brill
Associate
Washington, D.C.*

* Not admitted in D.C.; admitted only in New York; practice supervised by principals of Morrison & Foerster admitted in D.C.

FOLLOW US

Global Risk + Crisis Management Practice

John Carlin

Attorney Advertising

MORRISON FOERSTER

WHAT COMPANIES SHOULD BE DOING TO PREPARE FOR THE NEXT RANSOMWARE ATTACK

Adapted from CNBC article - http://www.cnbc.com/2017/05/17/the-wannacry-ransomware-attack-what-businesses-need-to-know-commentary.html

The "WannaCry" cyberattack that struck in May paralyzed businesses, government entities, and Britain's National Health Service, encrypting computer files on infected machines unless the owner paid a $300 ransom. The attack exposed major shortcomings in the approach of governments as well as businesses around the world to cybersecurity. And it reveals just how inadequate our existing approach to cybersecurity is in the face of the widespread availability of software exploits and the increasing prevalence of malicious actors online.

So what is a business that needs to act now to do? Putting in place a technically advanced cybersecurity system is expensive, and it requires constant, ongoing monitoring and investment. For years, Silicon Valley enthusiasts and business innovators have been telling us that "every company is now a tech company," but we are seeing almost weekly evidence now of something more insidious and challenging to corporate America: Every company, no matter what their core competency is supposed to be, is

continued on page 2

REDUCING AND MITIGATING HACKING RISKS

As many as 85% of targeted cyberattacks are preventable
through basic risk mitigation measures, according to the Department of Homeland Security.

Make sure you are constantly updating software. That also means keeping current with the latest operating systems.

Install appropriate security patches. You may not know until it is too late whether an update is a critical cybersecurity measure or whether it just adds some new feature or fixes an obscure bug in the software - so just update it!

Run "red team"-type testing by sending fake phishing e-mails out to employees and seeing how many people fall for them. Then, follow up with better training after they've accurately diagnosed the extent of their vulnerability.

Limit computer admin functions based on users' duties. This may limit malware's acess to and ability to infect your network.

Source: https://www.us-cert.gov/ncas/alerts/TA15-119A

now a tech company when it comes to cybersecurity. Your ability to conduct business, to do whatever the thing is you're actually supposed to be doing, is contingent upon the strength of your technology systems and the resilience of your data systems.

That's the bad news. The good news is that we already know how to fortify systems against the WannaCry threat. Like so much of the malicious activity on the internet, the attack took advantage of known vulnerabilities. Back in March, Microsoft had in fact pushed out a patch to the vulnerability that the WannaCry ransomware was able to exploit. The problem was that many businesses and institutions hadn't applied the patch—and on a broader level many institutions consistently lag behind in updating their software or continue to use older operating systems that aren't supported by new security updates. While no set of defenses can be guaranteed to withstand a sustained attack from a sophisticated attacker, they can still go a long ways toward reducing and mitigating risk: according to the Department of Homeland Security, as many as 85% of targeted cyberattacks are preventable through these basic risk mitigation measures.

There are other things businesses can do to get ahead of the curve.

- First, every business should examine what it is doing to protect against phishing attacks. Warning and educating employees about these threats is obviously a good idea—but a more effective tactic is to run a "red team"-type test by sending fake phishing e-mails out to employees and seeing how many people fall for them. Companies can then follow up with better training after they've accurately diagnosed the extent of their vulnerability.

- Second, as the WannaCry attack shows, it's imperative for businesses to make sure they are constantly updating their software and installing appropriate security patches. That also means keeping current with the latest operating systems. Oftentimes, a patch might only work with the most current system, leaving older ones in a state of ever-worsening security limbo (as has been the case with Windows XP).

- Third, the ransomware attack carries another important, related lesson: the patch that Microsoft had pushed out in March did not have a large red sign next to it that said "URGENT Patch Needed To Prevent Against Devastating Ransomware Attack." The update was offered quietly without a further description. Whatever the reason for this (and perhaps it was because Microsoft didn't want to alarm users or call attention to the vulnerability), the fact remains that you may not know until it is too

continued on page 3

late whether an update is a critical cybersecurity measure or whether it just adds some new feature or fixes an obscure bug in the software.

- Finally and maybe most critically, companies should game out these cyber scenarios and have a plan in place for how to handle them. Every business (whether in the tech sector or not) should consider what its worst-case cyber event would look like and how that event would be handled. What corporate governance structures would kick in, and are there ways to elevate problems directly to the CEO? Does the legal department have the right kind of relationship with the IT people so that the lawyers can understand what's going on? Companies should also consider—in advance—what their policy should be for notifying law enforcement. And, in the event of a ransomware attack, they should consider whether they would heed the FBI's advice not to pay in all cases or would be willing to take some other approach if their business depended on it.

Without question, these decisions are complicated, and there is probably no one-size-fits-all set of answers. The legal fallout can also be sprawling—ranging from possible consumer-privacy litigation, to shareholder suits, to cooperating in criminal investigations. The ramifications can even include being drawn into an international incident with a foreign adversary, as was shown by the Sony hack in 2014—and as current reporting is suggesting may be the case here. A business that falls victim to an attack also likely won't know who is behind the attack for some time, and so will be forced to make these decisions with imperfect information about whether it is dealing with ordinary crooks, a hostile nation-state, a terrorist organization, or a combination of these actors working in concert.

Every business (whether in the tech sector or not) should consider what its worst-case cyber event would look like and how that event would be handled.

Planning for these scenarios and putting safety measures in place may sound expensive and onerous. But as recent events make clear, the cost of not preparing for them can be far higher. And unfortunately, businesses cannot count on governments to do this work for them. While federal agencies continue to assess their own vulnerabilities—and write the many reports that the recent executive order prescribes—the private sector must harness its own abilities to adapt and innovate in order to be better prepared for the next attack.

ZTE RESOLUTION MAY SIGNAL NEW ADMINISTRATION'S APPROACH TO SANCTIONS ENFORCEMENT

Adapted from CNBC article - http://www.cnbc.com/2017/03/14/the-us-just-fired-a-1-billion-warning-shot-with-massive-fines-against-chinese-telecom-firm-commentary.html

On March 22, ZTE Corporation, the large Chinese telecommunications equipment firm, pleaded guilty in the Northern District of Texas to criminal export-control violations and accepted a combined penalty from U.S. regulators that could total as much as $1.19 billion. As recounted in a Department of Justice (DOJ) press release, ZTE's guilty plea—to charges including willfully conspiring to violate the International Emergency Economic Powers Act (IEEPA)—stemmed from a long-running criminal scheme in which ZTE sent controlled equipment and technology that originated in the United States to Iran and took elaborate steps to conceal the true nature of these transactions from the forensic accounting firm retained by outside counsel to examine ZTE's sanctions compliance. The guilty plea was announced alongside settlements with the Department of Commerce and Treasury that the government said at the time may add up to "the largest fine and forfeiture ever levied by the U.S. government in an export control case."

When the government announces a resolution of this scale, its public statements are carefully crafted to communicate the priorities of regulators. The ZTE matter is by far the most significant sanctions enforcement action announced under the new administration, and we see three key takeaways for multinational companies and their counsel.

- First, the price tag of resolving the ZTE matter should underscore to boardrooms worldwide the continued importance of a well-functioning compliance program and the pitfalls of an insufficient response to indications of wrongdoing. The Commerce Department reportedly began investigating ZTE following news stories in Reuters in 2012 that the company was illegally shipping U.S. hardware and software to Iranian telecommunications carriers. Yet ZTE resumed illegal sales to Iran even after outside counsel had been retained in connection with an ongoing grand jury investigation, and the criminal charges against ZTE were predicated in part on efforts to deceive the forensic accounting firm and defense counsel representing the company during the course of that investigation. As part of the plea, ZTE agreed to accept a lengthy period of corporate probation and the appointment of an independent compliance monitor. (Indeed, in a move that drew

continued on page 4

notice, Judge Kinkeade modified the proposed plea agreement to ensure that the court retained control over the monitor, including adding language referring to the monitor as a "judicial adjunct.") The focus in the plea agreement on establishing an effective compliance structure at ZTE going forward highlights the costs of not getting it right the first time.

- Second, the DOJ release announcing the ZTE resolution pointedly stated that it resulted from an "all of government approach to sanctions enforcement," a trend that multinational commercial and industrial companies that navigate U.S. sanctions and export control regimes would do well to take note of and prepare for accordingly. The spectrum of consequences across criminal and civil authorities was as striking as the total dollar amount of the settlement. A senior DOJ official told reporters that the Commerce Department's decision to add ZTE to the BIS Entity list, effectively cutting them off from U.S. suppliers, was "the game-changing event in the case" that led the company to change course and produce key documents and witnesses. With authorities across the U.S. government working collaboratively to bring every tool to bear in investigations and enforcement matters, the risks for companies facing even a civil investigation—even those outside the financial sector and other tightly regulated industries—can be staggering. Increasingly, the ramifications of civil enforcement may prove to be as steep as criminal penalties.

- Third, the whole-of-government approach to sanctions enforcement merits close watching for the additional reason that it may portend how the new administration will pursue other policies in the national security arena affecting multinational businesses, including reviews of foreign investments in U.S. entities and the response to the growing cyber threat. In recent years, the U.S. government has made a number of significant organizational changes to better integrate sanctions enforcement with other national security tools and authorities. In 2014, for example, the DOJ reorganized the National Security Division (which one of us led until recently) to create a new position overseeing the protection of national assets, including efforts to combat economic espionage, proliferation, and cyber threats to national security. A whole-of-government approach can be particularly critical as a way to engage the cyber threats, in which difficult challenges such as establishing attribution will often require close collaboration among departments and agencies. While it is only an early indication, the resolution of the ZTE matter represents a sign that the new administration may continue this effort.

RUSSIA WILL BE BACK TO MEDDLE IN OUR ELECTIONS AGAIN: WHY AREN'T WE MORE PREPARED?

Our intelligence community has repeatedly warned the American people that Russia will come back to meddle with our elections again. We recently saw the final leg of the French presidential election marred by massive leaks of candidate Emmanuel Macron's campaign files and emails—the result of a cyberattack news reports quickly attributed to the same Russian-backed hackers who sought to interfere in the U.S. election last year. The controversy after the firing of FBI Director James Comey should be the final straw that makes clear why the United States needs a new approach to countering foreign threats to our election system.

As Director of National Intelligence James Clapper warned earlier this month, in a statement that only takes on greater urgency in the wake of Comey's firing, "If there has ever been a clarion call for vigilance and action against a threat to the very foundation of our democratic political system, this episode is it." Yet, without quick action, we appear destined to relive the same events in the next election cycle.

One lesson as people look back on last year's unprecedented events is clear: the decisions made by good people trying to do the right thing for the right reasons led to bad outcomes. It's clear we need a new mechanism that preserves the public's trust while protecting our democracy. That's why we should consider something akin to a "dead man's switch" for our electoral process that ensures decisions around election tampering are automatically removed from politics—and that retaliation for such attacks is also prescribed in advance. This begins with mapping out a nonpartisan process in advance, one that relies on the career government intelligence professionals and analysts whose careers have been spent drawing conclusions about foreign motives, and then, in response, uses the tools we already have at our disposal to respond.

To begin, we should designate in advance that a body like the National Intelligence Council, the group of career analysts who help issue consensus national intelligence assessments, agrees with a high degree of confidence that if a foreign power—Russia or any other country that watched 2016 unfold and now thinks that it can mess around in our democracy with little cost—is trying to influence the election or undermine confidence in it, that finding should trigger an agreed upon set of actions, potentially both covert and overt.

continued on page 5

This analysis and conclusion can and should be conducted entirely removed from political appointees, just as at the Justice Department where there is a tradition of deferring to career professionals and prosecutors making sensitive decisions around political corruption cases to avoid an actual or the appearance of a conflict of interest. We cannot allow our response to be sidetracked by partisan politics. Analogizing to Article 5 of the NATO treaty, which sees an attack on one country as an attack on the whole alliance, Senator Lindsey Graham has called for bipartisan agreement in advance that "an attack on one party is an attack on all."

The message must be clear to foreign adversaries long before we approach our next election: any attempt to attack our campaigns, our candidates, or our voting systems will be met with prompt and strong retaliatory action.

Once the intelligence community concludes that a foreign power is seeking to meddle in an election, there is a playbook we can follow. The United States has shown in recent years the many weapons we have in our arsenal for responding to cyberattacks from foreign nations, including public condemnations, international sanctions, the expulsion of foreign diplomats, and even the filing of criminal charges. These responses have already helped shape the behavior of adversaries like North Korea, China, and Iran, and we should make more use of them in the future, as well as additional covert methods.

President Obama took many of these actions after the election, leveling sanctions, expelling Russian diplomats, and closing Russian compounds inside the United States, but it is clear in retrospect that the response should have come sooner. In the future, particularly if procedures are worked out in advance, the United States could lead decisive multilateral action with other western democracies at the first sign of interference, as allies like France, the United Kingdom, and Germany all share our interest in promoting democratic institutions and keeping foreign actors out of our elections.

The message must be clear to foreign adversaries long before we approach our next election: any attempt to attack our campaigns, our candidates, or our voting systems will be met with prompt and strong retaliatory action. Anything less than that might encourage Russia, China, or any other foreign adversary to think they can come after us with impunity.

Public education also matters: the more we discuss these threats openly now and in the future, the better prepared American voters will be to understand these attacks if they happen in the next year during the congressional midterms or going into the 2020 presidential election. We've seen the acrimony these events can create and how a failure to work out these issues in advance risks miring the response in partisan debate. And that, unfortunately, plays right into Russia's hand, sowing doubt about the trustworthiness of our government and our leaders. We must heed the warnings while we can. As Clapper said in his testimony before Congress, "I hope the American people recognize the severity of this threat and that we collectively counter it before it further erodes the fabric of our democracy."

SECOND CIRCUIT MICROSOFT CASE MAY BE HEADED TO U.S. SUPREME COURT

The Department of Justice will soon decide whether to ask the Supreme Court to overturn a major cyber-related ruling from a lower court last year. What happens next could have big ramifications for the U.S. technology sector and provide an early indication of how the new administration intends to navigate competing demands from law enforcement and privacy advocates.

At stake is a much-discussed decision in which a three-judge panel of the Second Circuit Court of Appeals—a prominent federal appellate court that hears cases in New York—refused to uphold a federal warrant directing Microsoft to turn over user account information to the DOJ. Had the data been stored in the United States, there is no question that Microsoft would have had to comply. But because the data was stored on an overseas server, the Second Circuit concluded the warrant went beyond the authority of the Stored Communications Act (SCA) notwithstanding probable cause that the account was being used in furtherance of a U.S. crime.

The outcome was quickly hailed by technology companies and privacy advocates. Microsoft's chief legal officer praised the Second Circuit's decision as "a major victory for the protection of people's privacy rights under their own laws rather than the reach of foreign governments." And an attorney for the Center for Democracy and Technology, a non-profit that advocates for greater internet privacy, told *Wired* that had Microsoft lost the case, it "would have prompted foreign governments to insist that their process reaches data stored inside the United States. It would have been like the Wild West." In the wake of the decision, Google and other tech companies—as well as privacy advocates—have sought to defend and expand on it in courts across the country.

continued on page 6

At the same time, the ruling caused serious heartburn for many in law enforcement because it left the availability of a critical tool dependent on where the suspect's data happens to be stored. Even one of the Second Circuit judges who sided against the DOJ conceded that its implication was that a U.S. company could "thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing . . . to store them on a server in another country."

Since the decision came down last year, the DOJ has gone to great lengths to cut it back. In a strongly worded brief, the DOJ asked the full Second Circuit to set aside the decision, warning that it "significantly limit[s] an essential investigative tool used thousands of times a year, harming important criminal investigations around the country, and causing confusion and chaos among providers as they struggle to determine how to comply." While that effort fell one vote short (a 4-4 tie), the DOJ continued to press these arguments in other courts in the hopes of a different outcome. To some degree, this latter strategy has worked, including two recent cases involving Google in which lower courts ruled in DOJ's favor, declining to extend the Second Circuit's approach.

Notably, much of that litigation occurred against the backdrop of an eight-member court Supreme Court and before senior officials from the new administration were up and running. Now, with Justice Gorsuch confirmed and the new Attorney General and Deputy Attorney General in place, the administration will need to evaluate carefully the risks and benefits of enlisting the Supreme Court's review. Earlier this year, the DOJ received an extension of time to ask for Supreme Court review until May 24 and recently received a further extension until June 23.

At the same time, if the Administration lets the Second Circuit decision stand (at least for now), it will mean denying the DOJ access to information that could be critical to uncovering and prosecuting serious crimes.

The federal government would generally prefer to have a favorable ruling in hand from another Court of Appeals before heading to the Supreme Court, particularly in a big case involving new technology and complex issues. Moreover, all of this is taking place at a time of renewed public scrutiny of the SCA as a whole that may lead Congress to make broader changes. (In his confirmation hearing, Attorney General Sessions was asked by Senator Hatch whether he would work with Congress on a statutory change to address the Second Circuit ruling and answered that he would.)

At the same time, if the Administration lets the Second Circuit decision stand (at least for now), it will mean denying the DOJ access to information that could be critical to uncovering and prosecuting serious crimes. In addition, investigators and private companies will potentially be subject to different sets of rules depending on where the judge in their case is located. There is also a risk that the ruling will create incentives for "data localization" regimes in which countries insist that data pertaining to its nationals is stored locally at the cost of efficiency, innovation, and, in many countries, free expression.

Whatever the Administration—and potentially the Supreme Court—decides, the case bears close watching in the weeks and months ahead as the Second Circuit ruling continues to have serious implications not just for the government but for the U.S. companies that store data and interact with regulators overseas.

FOREIGN INVESTMENT IN CRITICAL TECHNOLOGIES FACES ENHANCED SCRUTINY: THE TRUMP ADMINISTRATION MAY EXPAND FOCUS TO ADDRESS CHINESE ACTIVITIES IN SILICON VALLEY AND PERCEIVED ECONOMIC IMBALANCES

Foreign investment—and in particular Chinese investment—in U.S. science and technology sectors has increased significantly in recent years, a development that has not escaped the attention of the White House and U.S. national security officials. We already saw indications of a policy shift under President Obama, and the Trump administration and Capitol Hill are indicating that they might pursue broader policy changes. Consider these developments:

- The U.S. government is reportedly looking to strengthen the role that the Committee on Foreign Investment in the United States (CFIUS) can play in reviewing Chinese investments in fields such as artificial intelligence and machine learning technologies. CFIUS is the interagency committee charged with reviewing foreign investments and advising the president on their impact on national

continued on page 7

security. According to a recent report by Reuters, Pentagon and other administration officials are concerned that Chinese companies are investing in these new technologies in a manner that does not currently trigger CFIUS review, particularly given that AI and machine learning technologies could potentially be applied for military uses (for example, with respect to image recognition techniques and drone warfare).

- Meanwhile, Senator John Cornyn (R-TX) is reportedly working on a legislative proposal that would require heightened scrutiny where investments originate from countries posing certain national security risks, as well as a mechanism for the Pentagon to designate certain technologies to receive a stricter level of review when foreign entities make investments. Senator Chuck Schumer (D-NY) may also be preparing legislation that would require CFIUS to consider economic factors in addition to national security risks in conducting its reviews.

- These developments are part of a broader trend under which technologies designed and built by startup companies in Silicon Valley may increasingly overlap with potential military uses and other U.S. national security concerns. The military "supply chain," for example, may no longer be limited to traditional sectors such as aerospace or weapons; it could also include technologies such as machine learning platforms, even if those technologies are initially developed for purely private-sector uses. Overseas investment in new technology startups could also provide a potential avenue for foreign actors to access sensitive data regarding U.S. persons or to penetrate networks and systems that later incorporate the technology under development.

- With respect to Chinese investments in particular, a study released in December 2016 found that, since 2009, at least nine Chinese acquisitions fell through as a result of scrutiny (or the prospect of scrutiny) from CFIUS. And when the congressionally established U.S.-China Economic and Security Review Commission issued its 500+ page Annual Report for 2016, the report made a pointed recommendation that "Congress amend the statute authorizing [CFIUS] to bar Chinese state-owned enterprises from acquiring or otherwise gaining effective control of U.S. companies."

- In January 6, 2017, President Obama's Council of Advisors on Science and Technology released a report concerning the United States' status as the long-term leader in semiconductor technology that highlighted China's efforts to "reshape the market in its favor" by investing billions of government-backed dollars in bolstering its position as a leader in the global semiconductor market. While recognizing that reflexively opposing Chinese investment may not be in the best interests of the United States, the report emphasized that some acquisitions of U.S. semiconductor companies may "pose[] intolerable national security risks that cannot be mitigated through steps short of stopping their acquisition."

It remains to be seen what type of legislative proposal (if any) the Trump administration may ultimately put forward. Renegotiating the bilateral relationship between the United States and China was obviously a constant refrain of President Trump's 2016 campaign, leading many to predict that government officials in the new administration may attempt to implement a policy that prioritizes "fair trade" and that focuses on American workers and families over free trade, at least in cases when the two priorities conflict. In particular, President Trump and his transition team made statements suggesting that his administration's policies toward foreign direct investment from China are likely to be viewed transactionally, with a focus on ensuring equal treatment for U.S. companies that operate in China.

9: the number of Chinese acquisitions that failed as a result of CFIUS scrutiny

As noted above, both Senators Cornyn and Schumer are reportedly preparing legislation that would expand CFIUS's authorities—though Senator Cornyn's proposed legislation would continue to maintain CFIUS's focus on national security issues, whereas Senator Schumer's could sweep in broader economic issues. Observers in this area also took note of Treasury Secretary Steven Mnuchin's testimony at his confirmation hearing that he would work with Congress "to review, moderniz[e], and potentially expand [CFIUS's] powers as needed in respect to [the review of investments from state-owned enterprises]." However, Secretary Mnuchin also said more recently that he believes CFIUS should remain focused on national security issues and that economic issues respecting trade with China should be dealt with separately. Additionally, Defense Secretary James Mattis recently stated that he believes CFIUS is "outdated" and that "[i]t needs to be updated to deal with today's situation." No legislation has been formally introduced in Congress as of this writing.

There is also the possibility of policy changes even in the absence of legislation. Although CFIUS may lack express statutory authority to review transactions from a strictly economic perspective, CFIUS already construes its jurisdiction broadly, and the term "national security" is arguably vague enough to permit an even more expansive

continued on page 8

interpretation that encompasses some economic impacts even in the absence of a statutory change. Alternatively, or in addition, the Trump administration may try to use its considerable discretion under statutes such as the International Emergency Economic Powers Act (IEEPA) to restrict certain transactions involving foreign entities.

THE NEW ADMINISTRATION'S EXECUTIVE ORDER ON CYBER SECURITY: KEY TAKEAWAYS FOR INDUSTRY

On May 11, the Trump administration issued a much-awaited executive order on cybersecurity. The order recognizes some critical truths about the security of the federal government's networks—including that "[t]he executive branch has for too long accepted antiquated and difficult-to-defend IT." It orders agencies across the government to assess the risks and vulnerabilities they face and, importantly, to start taking steps to consolidate and modernize the government's systems.

The order also seeks to address vulnerabilities in private industries, and particularly in critical infrastructure entities, but its scope is limited. The Department of Homeland Security (DHS), in concert with other agencies, is directed to look into legal authorities or other capabilities that federal agencies could use to support cybersecurity of critical infrastructure entities. That might mean greater attempts at regulation, though it could also entail voluntary cooperative efforts and more information sharing. Interestingly, DHS is also directed to examine whether critical infrastructure entities are sufficiently transparent about their cyber risk management practices, and whether federal policies and practices could do more to promote market transparency.

There are three other points of interest for industry:

- First, the order announces a broad effort to improve internet security against threats perpetrated by automated and distributed attacks, such as attacks by botnets. While the order does not require private companies to do anything, it directs the Secretaries of DHS and Commerce to identify appropriate stakeholders and "promote" actions in order to reduce these cyber threats. Within a year, DHS and Commerce are required to submit a report on these efforts to the president.

- Second, the order brings much-needed focus to the security of our electrical grid, directing the Secretaries of Energy and DHS to assess the potential for a prolonged power outage that could be caused by a cyberattack and any shortcomings in the government's ability to handle such a situation, or at least to mitigate the consequences.

- Third, various cabinet-level national security officials are directed to draw up a report on cybersecurity risks facing the defense industrial base, including its supply chain. So the defense industry can likely expect to engage with the government on this effort.

All told, the order directs government agencies to write more than a dozen reports—many of which are due within 90 days or sooner. Some have been critical of this heavy focus, noting that the order doesn't actually allocate funding to improve cybersecurity or direct government agencies or the private sector to change any practices. But those types of measures may well require legislation. For now, we can expect the government—and particularly DHS—to be quite busy in scoping out the various risks identified in executive order, engaging with private industry, and potentially proposing more prescriptive measures down the road.

SUPREME COURT TO DECIDE WHETHER CORPORATIONS CAN BE HELD LIABLE UNDER THE ALIEN TORT STATUTE

The Supreme Court agreed in April to decide whether the Alien Tort State (ATS) categorically forecloses corporate liability. The case, *Jesner v. Arab Bank*, PLC, will be heard next fall and will determine whether corporations can be sued under a centuries-old law that gives U.S. federal courts jurisdiction to hear suits brought by aliens for torts "committed in violation of the law of nations or a treaty of the United States."

The role and meaning of the ATS has been the subject of much debate in recent years. Rights groups began using the statute in late 1970s to sue individuals alleged to have committed human rights violations, oftentimes where the principal events took place overseas. Corporations—both foreign and domestic—have also at times been named as defendants.

The Supreme Court initially set out to decide whether corporations can be sued under the law in 2011, when it granted certiorari in *Kiobel v. Royal Dutch Petroleum*. In that case, Nigerian nationals residing in the United States sued a set of Dutch, British, and Nigerian oil corporations, alleging that they aided and abetted the Nigerian Government in committing human rights violations. The Second Circuit dismissed the complaint, finding that the corporations could not be sued under

continued on page 9

the ATS because the "law of nations" does not recognize corporate liability. The Supreme Court received briefing and argument on this question but then changed its inquiry to whether the ATS allows courts to hear suits where the alleged wrongdoing has occurred abroad. After a second round of briefing and argument, the Court held that the ATS barred the plaintiffs' claims because "all the relevant conduct took place outside the United States." It left the question about corporate liability unanswered.

Jesner v. Arab Bank tees that question back up. The plaintiffs in the case are foreign victims or family members of victims of terrorist acts that took place in Israel, the West Bank, and the Gaza Strip. The alleged wrongdoing, however, aims to focus on conduct that occurred in the United States: the plaintiffs claim that Arab Bank (which is based in Jordan and has branches around the world) used its New York branch to finance the terrorist groups responsible for the attacks. When the case reached the Second Circuit, the court adhered to its prior holding that the ATS does not allow claims against corporations—though it suggested that the Supreme Court could be open to a different view.

In petitioning the Court for certiorari, the plaintiffs noted that multiple other courts of appeals (including the 7th, 9th, 11th, and D.C. Circuits) have held that the ATS allows corporate liability. They further maintained that corporations are capable of committing acts that constitute traditional law-of-nations violations, as well engaging in terrorist activity. Additionally, they argued that when Congress enacted the ATS, it was already well settled that corporations could be liable for torts.

In its response to the petition for certiorari, Arab Bank argued that the allegations do not have a sufficient nexus to the United States under *Kiobel*—and, therefore, that the Court could again find itself not reaching the corporate liability question even if it took the case. (The brief also devoted significant space to arguing that Arab Bank does not finance terrorist activities and is a positive force for economic development and security in the Middle East.) Additionally, Arab Bank's response argued that the corporate liability question is of diminishing importance because, in the wake of *Kiobel*, many ATS suits have been dismissed on the grounds that they raise extraterritorial claims.

The role and meaning of the ATS has been the subject of much debate in recent years.

The Court deliberated for several months before deciding to grant the case. It presumably intends to reach the merits of whether the ATS allows corporate liability, though Arab Bank can be expected to maintain that the suit should be dismissed either way because the real alleged wrongdoing occurred overseas. If the Court rules for the petitioners, that would leave the door open for other ATS suits against multinational corporations with a U.S. presence, provided that at least some of the alleged conduct occurred in the United States. The case will be argued next fall and should be decided within the next year.