Bloomberg BNA

BNA's Patent, Trademark & Copyright Journal®

TRADE SECRETS

Attorneys from Morgan, Lewis & Bockius, in the sixth installment in a series of articles examining trade secrets issues in the U.S., outline actions a company can or should take when seeking remedies after its trade secrets have been hacked.

What Legal Options Does Your Company Have After Your Trade Secrets Are Stolen by Cyber Espionage or Cyber Attack?

By Mark L. Krotoski and David I. Miller

Mark L. Krotoski is a Litigation Partner in the Privacy and Cybersecurity and Antitrust practices of Morgan, Lewis & Bockius. He previously served as the National Coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division of the U.S. Department of Justice.

David I. Miller is a Litigation Partner in the White Collar, Investigations, and Securities Enforcement practices of Morgan, Lewis & Bockius. He previously served as an Assistant U.S. Attorney in the Southern District of New York, a terrorism prosecutor with the Department of Justice, a Special Assistant U.S. Attorney in the Eastern District of Virginia, and as Assistant General Counsel for the Central Intelligence Agency.

The authors wish to recognize the contributions of Matt Ladd, an associate of the firm.

Assume that you are general counsel of a growing U.S. company. You just learned that your company was hacked and valuable trade secrets and other confidential business information were stolen. The source of the attack could be a foreign government, an organized cyber syndicate, or an insider who recently left to work with a competitor. But, initially, the source is unknown.

How do you respond? What are your legal options? What might the government do to assist you? This article reviews and highlights key issues to consider in this recurring scenario.

Cyber Espionage and Cyber Attacks on U.S. Companies Are a Serious Threat

Cyber espionage and cyber attacks can take many serious forms. FBI Director James B. Comey, Jr. has identified four key sources:

> sophisticated cyber threats [are] from [1] state-sponsored hackers, [2] hackers for hire, [3] organized cyber syndicates, and [4] terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us.[1]

Consider several recent developments demonstrating how cyber attacks present a serious threat for private industry and U.S. national security:

- On April 1, 2015, the White House issued an Executive Order declaring that cyber espionage has be-

[1] Statement of James B. Comey, Jr., FBI Director, Senate Judiciary Committee, Oversight Of The Federal Bureau Of Investigation, at 4 (May 21, 2014), http://www.judiciary.senate.gov/imo/media/doc/05-21-14ComeyTestimony.pdf.

come a ''national emergency,'' and authorizing the imposition of sanctions in appropriate cases against individuals and entities engaged in ''malicious cyber-enabled activities,'' including for ''causing a significant misappropriation of . . . trade secrets.''[2]

■ In February 2015, Defense Secretary Ashton B. Carter, on the eve of his recent confirmation, told the Senate Armed Services Committee that the ''Department should continue to take strong actions to address China's use of cyber theft to steal U.S. companies' confidential business information and proprietary technology.''[3]

■ In December 2014, the FBI announced that it had attributed cyber attacks on Sony Pictures Entertainment to the North Korean government.[4]

■ In May 2014, five members of the Chinese military were charged with economic espionage, computer hacking and several other offenses.[5] Attorney General Eric Holder noted the case ''represents the first ever charges against a state actor for this type of hacking.''[6]

■ Other reports of state-sponsored hacking and misappropriation have been traced to Chinese and Russian government groups.[7]

■ Recent congressional hearings have focused on the problem of cyber espionage and attacks on U.S. businesses.[8]

Clearly, we have entered a new era where U.S. companies are being targeted persistently for cyber theft by domestic and foreign actors.

Mitigating the Loss and Navigating Legal and Technical Issues

After a company is the victim of a cyber attack, its highest company priorities are recovering its trade secrets; ensuring that the trade secrets and confidential information are not used; addressing potential reputational harm and the loss of business or customers; and minimizing any adverse publicity resulting from media coverage and legal consequences. While the company certainly wants to resume normal business operations quickly, it nevertheless faces a host of legal and technical issues. Some of the initial legal issues may include fulfilling data breach notification requirements among 47 states,[9] assessing the scope of any cyber insurance coverage, and responding to class action law suits. If the attackers are outside the United States, international avenues to obtain evidence and pursue a claim will be needed.

For public companies, there may be SEC disclosure requirements concerning the loss of intellectual property or other company assets from cyber espionage or cyber attack. In October 2011, the Securities and Exchange Commission specifically advised:

> [I]f material intellectual property is stolen in a cyber attack, and the effects of the theft are reasonably likely to be material, the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition.[10]

The company will also likely need to engage an experienced forensic firm that can address the specific technical needs raised by the compromise. In most cases, the attorney-client privilege covers the initial investigation by the forensic firm that works closely with outside counsel in assessing the scope of, and mitigating the damages caused by, the cyber attack. If the government is also conducting an investigation, the company will need to coordinate closely with law enforcement to ensure that evidence is properly preserved. Companies should be aware, however, that the voluntary disclosure of investigative information to the government may result in the disclosure of otherwise privileged material. This may affect a privilege waiver with respect to future lawsuits.[11]

---

[2] Exec. Order, ''Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities'' (Apr. 1, 2015), https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m. *See also* Corie Bennett & Elise Viebeck, *Obama declares cyberattacks a 'national emergency,'* THE HILL (Apr. 1, 2015), http://thehill.com/policy/cybersecurity/237581-obama-declares-cyberattacks-a-national-emergency.

[3] Advance Policy Questions for the Honorable Ashton Carter Nominee to be Secretary of Defense (Q249), at 70, http://www.armed-services.senate.gov/imo/media/doc/Carter_APQs_02-04-15.pdf.

[4] Press Release, Federal Bureau of Investigation, Update on Sony Investigation (Dec. 19, 2014), http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation); *see also* Advance Policy Questions for the Honorable Ashton Carter Nominee to be Secretary of Defense (Q172), at 49 (referring to the cyber attack by North Korea), http://www.armed-services.senate.gov/imo/media/doc/Carter_APQs_02-04-15.pdf.

[5] Robert Anderson, Press Conference Announcing Charges Against Five Chinese Military Hackers, U.S. Dep't of Justice (May 19, 2014), http://www.fbi.gov/news/speeches/combating-state-sponsored-cyber-espionage.

[6] Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[7] *See, e.g.*, Mandiant: *APT1 Exposing One of China's Cyber Espionage Units* (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; FireEye, *APT28: A Window Into Russia's Cyber Espionage Operations*?, at 3 (2015), https://www2.fireeye.com/apt28.html.

[8] *See, e.g.*, Cyber Espionage And The Theft Of U.S. Intellectual Property And Technology: Hearing before the House Comm. on Energy and Commerce Subcomm. On Oversight and Investigations, 1st. Sess. 113th Cong. (July 9, 2013); Cyber Threats From China, Russia, and Iran: Protecting American Critical Infrastructure: Hearing before the House Comm. on Homeland Security Subcomm. On Cybersecurity, Infrastructure Protection, and Security Technologies, 1st. Sess. 113th Cong. (March 20, 2013).

[9] *See* Nat'l Conference of State Legislatures, Security Breach Notification Laws (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[10] SEC Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[11] This is a particular concern if the government is investigating the company for potential misconduct. *See In re Steinhardt Partners, L.P.*, 9 F.3d 230, 235-36 (2d Cir. 1993) (volun-

   ISSN 0148-7965

Considering the Legal Remedies

Depending on the nature of the intrusion, it may take some time to track and locate the hackers. Legal remedies may be pursued through two paths: civil remedies and/or a criminal prosecution.

Civil Litigation Options

If an individual or group is identified, they can be named in a civil complaint. In some cases, there may be some benefits to filing a so-called ''John Doe'' complaint before the perpetrators can be identified conclusively and the true name can be added later.[12] This step allows the use of the legal process to subpoena necessary information and stop the statute of limitations from running. While successful civil cases can be pursued, they are not without issues as shown below.

Civil Trade Secret Claims

Presently there is no private right of action for a federal theft-of-trade-secret claim. Consequently, such a claim must rely on state law. Presently, 48 states and the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted some form of the Uniform Trade Secret Act (UTSA).[13] Further, criminal remedies may be available under the Economic Espionage Act of 1996,[14] as noted below.

Congress is giving serious consideration to enacting legislation that would provide a federal private right of action for theft of trade secrets. While state law may be effective in dealing with local trade secret misappropriation, a federal private right of action would give trade secret owners an additional option to seek relief in federal court where the trade secrets were stolen and transported outside the state or country.[15] Until then, state law must be used to bring a trade secret claim, whether the claim is brought in state court or federal court on other jurisdictional theories.[16]

Civil Computer Fraud and Abuse Act Claims

The Computer Fraud and Abuse Act (CFAA), originally enacted in 1984,[17] is the primary federal anti-hacking statute. The CFAA provides for a civil private right of action for damages or equitable relief, along with potential criminal penalties.[18] The CFAA covers claims for hacking into a company's network.[19]

There is one potential wrinkle under the CFAA: where the trade secret misappropriation is based on insider conduct. There is presently a division among the circuits on whether the CFAA applies when a trusted employee steals the company's confidential information using the company's computer.[20]

Establishing Personal Jurisdiction

Any civil case requires sufficient allegations that the defendant is subject to personal jurisdiction. Personal jurisdiction requires a jurisdictional basis and service of process. Service of process, in particular, can usually be accomplished for individuals and entities in the United States.

Service of process, however, may be problematic if the hackers are difficult to locate overseas. Service of process on foreign individuals, corporations, and states or agencies of states is governed by Fed. R. Civ. P. 4 and the provisions of the 1965 Hague Service Convention. The Hague Service Convention, of which the United States is a signatory, requires member states to designate a ''Central Authority'' to accept requests for ser-

---

tary disclosure of attorney work product to government during adversarial investigation will generally waive privilege for that work product as to future parties). Notably, there is no *per se* rule prohibiting ''selective waiver'' such that the presence of a ''common interest,'' particularly where the company is a victim, could preserve the privilege as to future adversarial parties. *Id.* at 236. Nevertheless, unlike the work product doctrine, the attorney-client privilege is automatically waived once material is produced to a third party. *See, e.g., Kingsway Fin. Servs., Inc. v. Pricewaterhouse-Coopers LLP*, No. 03-5560, 2007 BL 49596, at *2-3 (S.D.N.Y. June 27, 2007). It bears mentioning that the Department of Justice, as a matter of policy, does not compel a company to waive attorney-client and work product protections. *See, e.g.*, USAM § § 9-28.720 (''Eligibility for cooperation credit is not predicated upon the waiver of attorney-client privilege or work product protection.''), 9-28.760 (Oversight Concerning Demands for Waivers of Attorney-Client Privilege or Work Product Protection By Corporations Contrary to This Policy), http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/28mcrm.htm#9-28.760. For a useful recent discussion of the protections provided by the attorney client privilege during a data breach investigation, see *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168 (M.D. Tenn. 2014).

[12] *See, e.g.*, Cal. Code of Civ. Proc. § 474 (allowing an unknown defendant to be ''designated . . . by any name, and when his true name is discovered, the pleading or proceeding must be amended accordingly'').

[13] Only New York and Massachusetts have not enacted some version of the UTSA. For a list of the jurisdictions adopting the UTSA, *see* Uniform Law Commission, Legislative Fact Sheet: Trade Secrets Act, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade Secrets Act. The UTSA was published in 1979 by the Uniform Law Commissioners, and amended in 1985. *See* http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act. For the UTSA as amended in 1985, *see* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

[14] *See* 18 U.S.C. § § 1831-1839.

[15] *See, e.g.*, M. Krotoski, The Time Is Ripe for a New Federal Civil Trade Secret Law, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 28 (Nov. 7, 2014) (89 PTCJ 28, 11/7/14) (identifying several reasons warranting a federal trade secret private right of action).

[16] *See, e.g.*, M. Krotoski, Reviewing the Challenges in Bringing a Federal Trade Secret Case Under Current Law, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 475 (Dec. 19, 2014) (89 PTCJ 475, 12/19/14) (discussing jurisdictional issues and challenges in bringing a trade secret case in federal court) [herinafter, ''Reviewing the Challenges in Bringing a Federal Trade Secret Case ''].

[17] 18 U.S.C. § 1030. Section 1030 was originally enacted in 1984. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified at 18 U.S.C. § 1030 *et seq*.).

[18] 18 U.S.C. § 1030(g) (civil private right of action). The private right of action was added in 1994. *See* Pub. L. 103–322, title XXIX, § 290001(b)–(f), Sept. 13, 1994, 108 Stat. 2097–2099.

[19] The most common hacking charge is under 18 U.S.C. § 1030(a)(5), although other CFAA provisions may apply depending on the facts.

[20] *See, e.g.*, M. Krotoski & B. Dahl, Stealing Trade Secrets and Confidential Information With Computers: Time to Resolve the Lingering Circuit Split, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 1142 (Feb. 27, 2015) (89 PTCJ 1142, 2/27/15) (reviewing circuit split).

vice through submission of a standardized form.[21] The Central Authority (designated in the U.S. as the Department of Justice) then arranges for service according to the laws of the member state. Member states may also permit international service by alternative methods, such as personal service or service by mail, which they designate in their Convention filing documents.[22] Service of process on states that are not members of the Hague Service Convention may require the filing of a letter rogatory—a formal request for a U.S. court to issue a judicial order to a court in the foreign country—under Fed. R. Civ. P. 4(f)(2)(B), a much costlier and lengthier process. Clearly, the procedural hurdles in serving process in an action against those individuals or groups that perpetrate a cyber offense can be extensive.

Extraterritorial Applicability

Even where service of process may be effected internationally, a plaintiff may face challenges concerning the extraterritorial reach of the applicable statute. While usually a substantial U.S. nexus can be shown in a data breach case, if such a nexus is lacking, the key question will be whether the relevant statute by which one brings a cause of action has extraterritorial applicability.[23]

This limitation was articulated recently by the Supreme Court in *Kiobel v. Royal Dutch Petroleum Co.*, in which the Court held that the presumption against extraterritoriality prevented courts from recognizing a cause of action under the Alien Tort Statute for certain overseas conduct.[24] In defining the scope of the presumption against extraterritoriality, *Kiobel* relied heavily on the Supreme Court's opinion in *Morrison v. Nat'l Australia Bank Ltd.*, which dismissed a suit against a foreign bank under the Securities Exchange Act by invoking the presumption against extraterritoriality: ''[w]hen a statute gives no clear indication of an extraterritorial application, it has none.''[25]

Through *Morrison* and *Kiobel*, the Supreme Court has placed clear and strict limits on the ability of U.S. courts to adjudicate conduct that occurs beyond national boundaries, limits that persist even when the claims ''touch and concern the territory of the United States.''[26] Accordingly, if hackers have acted against a company's interests abroad, and a necessary U.S. nexus is not apparent, the company may face an issue of whether the presumption against extraterritoriality precludes suit.

Weighing the Benefits of a Federal Criminal Investigation

While the authors have been privileged to have served as federal prosecutors on trade secret, hacking, national security, and complex white-collar cases, there are trade-offs in relying on law enforcement to investigate and solve the case. A company should weigh these factors carefully.

The government has a variety of tools at its disposal to investigate and prosecute those responsible for a breach, including:

- Substantial investigative resources, including the ability to request assistance from federal agents across the U.S.;

- Using legal process to preserve electronic records,[27] and on a showing of probable cause, obtaining search warrants for the contents of electronic records such as email accounts of suspected hackers;[28]

- Using legal process to seize websites that are selling illegal products or are used to further illegal activity such as hacking activity;[29]

- The ability to obtain evidence abroad based on a Mutual Legal Assistance Treaty request;[30]

- The ability to extradite based on extradition treaties with more than 100 countries;[31]

[21] *See* Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters art. 2, Nov. 15, 1965, 20 U.S.T. 361, T.I.A.S. No. 6638.

[22] *See* Hague Service Convention art. 11.

[23] For example, the CFAA was amended in 2001 to include an extraterritorial provision. 18 U.S.C. § 1030(e)(2)(B) (providing that the CFAA applies to a computer that ''is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States''); *see also* 147 CONG. REC. S10551 (noting amendment ''include[s] qualified computers even when they are physically located outside of the United States''). For a case considering the extraterritorial reach of the CFAA prior to the 2001 amendment, *see United States v. Ivanov*, 175 F. Supp. 2d 367, 374-75 (D. Conn. 2001) (''Congress has the power to apply its statutes extraterritorially, and in the case of 18 U.S.C. § 1030, it has clearly manifested its intention to do so.''). While the Economic Espionage Act contains an extraterritorial provision, it only applies to criminal cases. Congressional legislation could extend this provision to civil actions. 18 U.S.C. § 1837 (applicability to conduct outside the U.S.); *see also* H.R. Rep. No. 104-788, at 14 (1996) (''To rebut the general presumption against the extraterritoriality of U.S. criminal laws, this subsection makes it clear that the Act is meant to apply to the specified conduct occurring beyond U.S. borders.'').

[24] *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1669 (2013).

[25] *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010).

[26] *Kiobel*, 133 S. Ct. at 1669.

[27] 18 U.S.C. § 2703(f).

[28] 18 U.S.C. § 2703(a).

[29] *See* 18 U.S.C. § § 981 (general civil forfeiture), 982 (general criminal forfeiture), 1834 (criminal forfeiture under the EEA), 2323(a) (civil forfeiture for specified IP offenses), 2323(b) (criminal forfeiture for specified IP offenses); 28 U.S.C. § 2461(c) (authorizing use of civil forfeiture statute in criminal cases). For a recent case example, *see* Press Release, U.S. Dep't of Justice, Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road (Jan. 16, 2014), http://www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php.

[30] USAM, Criminal Resource Manual 276 (Treaty Requests), http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00276.htm; U.S. Dep't of State, 7 Foreign Affairs Manual § 962.1 (Mutual Legal Assistance in Criminal Matters Treaties), http://www.state.gov/documents/organization/86744.pdf; *see also* Reviewing the Challenges in Bringing a Federal Trade Secret Case, *supra* note 16 (noting ''in one foreign economic espionage case, federal prosecutors and investigators were able to obtain a Mutual Legal Assistance Treaty request for law enforcement officials in Germany who successfully recovered trade secrets in Germany and returned them to the United States'').

[31] *See* U.S. Dep't of State, Treaties in Force: A List of Treaties and Other International Agreements of the United States in Force on January 1, 2013 (listing treaties with each country including extradition treaties), http://www.state.gov/

  PTCJ ISSN 0148-7965

■ Seeking restitution in a criminal prosecution under the Mandatory Victims Restitution Act (''MVRA''),[32] which would include cybercrimes as ''offense[s] against property'' that are ''committed by fraud or deceit'';[33] under the MVRA, the court ''shall order restitution to each victim in the full amount of each victim's losses as determined by the court.''[34]

While the benefits to the company from the above investigative efforts may be substantial, some of the costs may include:

■ Loss of control over the timing of the investigation and criminal case proceedings; in some instances, cases may take several years to investigate and litigate;

■ Potential adverse publicity and reputational harm resulting from criminal proceedings;

■ Litigation consequences resulting from a public criminal trial; and

■ Possible privilege waiver issues from disclosing the company's internal investigation to the authorities.

Accordingly, while federal authorities have had tremendous success in prosecuting economic espionage, trade secret theft, and computer hacking cases, companies should consider the near term and long term consequences of federal criminal action. Set forth below are some of the statutes the criminal authorities may use in a prosecution involving cyber espionage or cyber attacks.

Economic Espionage Act

The Economic Espionage Act (EEA) of 1996 penalizes two sets of offenses involving the theft of trade secrets.[35] First, under Title 18, United States Code, Section 1831, the Act prohibits foreign economic espionage: the misappropriation of a trade secret with the intent to benefit a foreign government, foreign instrumentality, or foreign agent. Before any Section 1831 charges can be filed, however, authorities must obtain the approval of the Assistant Attorney General for the National Security Division.[36] Since 1996, 10 cases have been authorized for prosecution.[37] Second, Section 1832 penalizes more traditional trade secret offenses, specifically the misappropriation of a trade secret with the intent to convert it to the economic benefit of anyone other than the owner and to injure the owner of the secret. Federal prosecutors have prosecuted successfully both forms of offenses through the years.[38]

Computer Fraud and Abuse Act (CFAA)

Criminal charges may also be filed under the CFAA.[39] As a recent example, the Department of Justice announced that it has extradited a Russian national who was previously indicted ''for his alleged role in a data theft conspiracy that targeted major corporate networks, stole more than 160 million credit card numbers, and caused hundreds of millions of dollars in losses.''[40]

Identity Theft Statutes

Hackers that steal personal identifying information may be prosecuted for identity theft.[41] For example, Section 1028 prohibits a hacker's theft of identification materials, including copies of driver's licenses, insurance cards and passports, or the transfer of ''means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of'' federal, state, or local law.[42] ''Means of identification'' is defined to include any name or number that can be used to identify a specific individual, such as a social security number, date of birth, driver's license or other identification number.[43]

Section 1028A, entitled ''Aggravated identity theft,'' provides a consecutive mandatory term of imprisonment of two years for those who, in relation to an enumerated felony (such as mail, bank and wire fraud), knowingly transfer, possess or use a ''means of identification'' of another person.[44] Courts have interpreted this section to require that offenders know that they are using the information of another person. Section 1029 addresses ''Fraud and related activity in connection with access devices,'' and is commonly used to prosecute those who steal and use credit card information, which is the most commonly stolen information in cyber breaches.[45]

Serving a Foreign Corporation

If the perpetrator of the offense is a foreign corporate entity, serving the defendant in a criminal prosecution

---

documents/organization/218912.pdf; *see also* 18 U.S.C. § 3181 note (listing countries with bilateral extradition agreements with the United States).

[32] 18 U.S.C. § 3663A(a)(2).

[33] *Id*. § 3663A(c)(1)(A)(ii).

[34] *Id*. § 3664(f)(1)(A); *see also United States v. Coriaty*, 300 F.3d 244, 253 (2d Cir. 2002) (observing ''the statutory focus on the victim's loss and upon making victims whole''). As a recent restitution example, *see Pena v. United States*, No. 12-846, 2014 BL 246497, at *3, *8-9 (D.N.J. Sept. 4, 2014) (in a computer fraud prosecution concerning a hacking scheme involving several telecom companies, upholding a restitution order of over $1 million as part of a plea agreement).

[35] Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified as amended 18 U.S.C. § § 1831–1839).

[36] *See* USAM § § 9-59.100, 9-90.020.

[37] Statement of Randall Coleman, Assistant Director, Counterintelligence Division, Federal Bureau Of Investigation, before the Senate Judiciary Subcommittee On Crime And Terrorism, ''Economic Espionage And Trade Secret Theft: Are Our Laws Adequate For Today's Threats?'' (May 13, 2014) (confirming that since 1996 ''there have been 10 economic espionage'' cases under Section 1831), http://www.judiciary.senate.gov/imo/media/doc/05-13-14ColemanTestimony.pdf.

[38] For recent examples, *see* M. Krotoski, *Common Issues and Challenges In Prosecuting Trade Secret and Economic Espionage Act Cases*, 57 United States Attorneys' Bulletin 2-23 (Nov. 2009), http://www.justice.gov/sites/default/files/usao/legacy/2009/12/10/usab5705.pdf; Reviewing the Challenges in Bringing a Federal Trade Secret Case, *supra* note 16.

[39] *See* notes 17 and 18, *supra*.

[40] *See* Press Release, U.S. Dep't of Justice, Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States (Feb. 17, 2015), http://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states.

[41] There are a variety of federal criminal statutes addressing this conduct, but the most widely used are 18 U.S.C. § § 1028, 1028A, and 1029.

[42] 18 U.S.C. § 1028(a)(7).

[43] *Id*. § 1028(d)(7).

[44] *Id*. § 1028A(a)(1).

[45] *Id*. § 1029(c)(1).

may be difficult. For companies, the Federal Rules of Criminal Procedure require that a summons be served ''by delivering a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process.''[46] Rule 4 also contains a so-called ''mailing provision,'' requiring that the summons be ''mailed to the organization's last known address within the [federal] district or to its principal place of business elsewhere in the United States.''[47] Federal courts have split on the issue of whether the mailing provision is an element of service or merely a notice requirement. At least two courts interpreting Rule 4 have held that compliance with the mailing provision is mandatory for effective service of process.[48] In *United States v. Kolon Indus. Inc.*, however, a criminal suit for theft of trade secrets and obstruction of justice, the court held that the mailing requirement was a non-jurisdictional notice provision, and that service could be effected through proper delivery.[49] To hold otherwise, the *Kolon* court observed, would effectively immunize a foreign corporation from service under the Federal Rules of Criminal Procedure when that corporation has no mailing address in the United States and no domestic alter ego to receive the summons.[50]

Due to this ambiguity in Rule 4, the current mailing requirement may be on its way out. On Aug. 15, 2014, responding to pressure from the Department of Justice and the Federal Bar Council, the Judicial Conference Committee on Rules of Practice and Procedure published for notice and comment proposed amendments to Rule 4, which would eliminate the mailing provision and facilitate service on foreign individuals and companies.[51]

Sanctions and Executive Initiatives

In appropriate cases, the government can levy sanctions against foreign companies and governments, including those who initiate cyber attacks, under the International Emergency Economic Powers Act (IEEPA).[52] On Jan. 2, 2015, for the first time, the U.S. issued sanctions against a country—in this case, North Korea—for its illegal cyber activities. Specifically, the government enhanced its overall economic sanctions against North Korea in direct response to its ''destructive, coercive cyber-related actions during November and December 2014.''[53] Although the United States has not yet issued sanctions against any other country as a direct response to cyber espionage, it has recently been suggested that economic sanctions could prove effective against state-sponsored cyber attacks originating in China.[54]

More recently, the President issued an Executive Order on April 1, 2015 (entitled ''Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities'') declaring cyber espionage a ''national emergency,'' and authorizing targeted sanctions against individuals and entities engaged in ''malicious cyber-enabled activities.''[55]

Areas for Congressional Reform

Companies that are the victim of cyber espionage or attack have several remedial avenues they can consider, but Congress can and should redress some of the existing challenges for these avenues under current law, including:

- Enacting a federal private right of action for trade secrets, which will provide companies with the option to obtain relief in federal court;[56]
- Addressing the lingering circuit split on whether the CFAA applies to an employee who steals confidential proprietary information by using the company's computers;[57]
- Reforming service requirements for companies and individuals overseas;[58] and
- Providing extraterritorial relief for other statutes that private litigants can use for hacking offenses.[59]

The President renewed the focus on cybersecurity legislative reforms during his Jan. 20, 2015 State of the Union Address:

> ''No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids[. . . .] I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information.''[60]

---

[46] Fed. R. Crim. P. 4(c)(3)(C).

[47] *Id.*

[48] *See United States v. Pangang Grp.*, 879 F. Supp. 2d 1052, 1064-65 (N.D. Cal. 2012) (granting motion to quash summons for failure to comply with mailing provision); *United States v. Johnson Matthey PLC*, No. 06-169, 2007 BL 210078, at *2 (Utah Aug. 2, 2007) (same).

[49] *United States v. Kolon Indus. Inc.*, 926 F. Supp. 2d 794, 801-02 (E.D. Va. 2013), *aff'd*, No. 3:12-cr-137, slip op. at 2 (E.D. Va. Dec. 23, 2014); *see also United States v. Dotcom*, No. 1:12-cr-3, 2012 2012 BL 265527, at *1 n.1 (E.D. Va. Oct. 5, 2012) (observing in *dicta* that the mailing provision is likely a notice requirement, not a component of service).

[50] *Kolon Indus.*, 926 F. Supp. 2d at 800, 802 (''[I]f the mailing provision could not be satisfied, the putative offender could not be brought to court. . . . And, to read the second sentence to impose an obligation that could not possibly be satisfied would produce an absurd result.''). Even after *Kolon*, the *Pangang* court on rehearing affirmed its ruling that service under the Federal Rules of Criminal Procedure requires compliance with the mailing provision. *See United States v. Pangang Grp.*, No. CR-11-00573, slip op. at 10 (N.D. Cal. Apr. 8, 2013) (''the United States must be able to show that it has complied with the mailing requirement to effect service'').

[51] *See* Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure, 329-37 (Aug. 2014), http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.

[52] 50 U.S.C. § § 1701 *et seq*.

[53] Exec. Order No. 13687, 80 Fed. Reg. 819 (Jan. 2, 2015).

[54] *See* Zachary K. Goldman, *Washington's Secret Weapon Against Chinese Hackers*, Foreign Affairs (Apr. 8, 2013), http://www.foreignaffairs.com/articles/139139/zachary-k-goldman/washingtons-secret-weapon-against-chinese-hackers.

[55] *See* note 2 *supra*.

[56] *See* note 15 *supra*, and accompanying text.

[57] *See* note 20 *supra*, and accompanying text.

[58] *See* note 51 *supra*, and accompanying text.

[59] *See* notes 23 to 26 *supra*, and accompanying text.

[60] President Barack Obama, State of the Union Address (Jan. 20, 2015), https://www.whitehouse.gov/the-press-office/

   ISSN 0148-7965

A current legislative proposal, updated from an initial proposal of May 2011, would amend the CFAA and the Racketeering Influenced and Corrupt Organizations Act (RICO) to make cyber crimes prosecutable under RICO, increase penalties for CFAA violations, and further enhance the government's ability to investigate and prosecute computer crimes.[61] This is an important step Congress should take to provide these tools, when appropriate, against organized cyber syndicates and other groups.

Conclusion

The risk of cyber espionage and cyber attack to U.S. companies has increased significantly over the past several years. As summarized in this article, in the event of a cyber attack, there are a myriad of legal issues that may arise and navigating those waters can be a veritable minefield. The ability to understand and address these issues, and use available resources and legal remedies in a timely manner, can be critical in recovering from a damaging cyber assault.

2015/01/20/remarks-president-state-union-address-january-20-2015.

[61] *See* Updated Administration Proposal: Law Enforcement Provisions, § § 101, 103 (Jan. 13, 2015), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.