BY
DAVID Z. BODENHEIMER
AND GORDON GRIFFIN

PILLAGING *THE* DIGITAL TREASURE TROVES

THE TECHNOLOGY, ECONOMICS, AND LAW OF CYBER ESPIONAGE

Cloaked in the disguise of a corporate insider, the spy penetrates the outer perimeter, slips past the lurking guardians, cracks the interior vault, loots the corporate secrets—and then turns off the computer and gets another coffee after the high-technology heist. In today's age of rampant cyber espionage, bet-the-company secrets and billion-dollar technology may be stolen in seconds or exfiltrated for months before detection. And this threat is here and now—and huge:

> *President Obama*:
> [In 2008] alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion.[1]

> *NSA Director General Keith Alexander*:
> The ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history.[2]

> *Representative Rogers*:
> They are stealing everything that isn't bolted down, and it's getting exponentially worse.[3]

For this exponentially expanding topic, we will tackle four core questions about cyber espionage:

- What are the technologies targeted for cyber espionage?
- How do the cyberspies crack the digital defenses?
- What is the economic impact of cyber espionage and digital thefts?
- What are the legal implications for cybervictims?

What Are the Technology Targets for Cyber Espionage?

Perhaps the simplest test to identify espionage targets is to ask this: Do you have any technology or secrets worth stealing? If so, you are probably an espionage target. Intelligence reports,

corporate surveys, and other data have confirmed the broad spectrum of US technologies and secrets coveted by foreign nations and corporate competitors.

In a landmark report in 2011, the Office of the National Counterintelligence Executive (ONCIX) catalogued the technologies of greatest interest for cybertheft and economic espionage:

- Information and communications technology;
- Military technologies, including marine systems and aerospace;
- Civilian and dual-use technologies, including clean technologies and advanced materials and manufacturing techniques;
- Health care, pharmaceuticals, and related technologies; and
- Agricultural technology.[4]

More recently, the Defense Security Service (DSS) identified the "Top Targeted Technologies" as including among others: information systems; electronics; lasers, optics, and sensors; aeronautics systems; materials and processes; space systems; positioning, navigation, and time systems; marine systems; information security; and manufacturing processes.[5] Similarly, the Director of National Intelligence (DNI) led off his office's overall threat assessment with cyberthreat—among which he listed the loss of "proprietary technologies and sensitive business information" due to "cyber espionage activities."[6]

David Z. Bodenheimer, a partner in Crowell & Moring LLP's Government Contracts Group, heads the Homeland Security Practice and currently serves as the ABA's Section of Science & Technology Law Division Co-Chair (Security, Privacy, and Information Law), SciTech Committee Co-Chair (Homeland Security), and Public Contract Law Section (PCL) Committee Co-Chair (Cybersecurity, Privacy, and Data Protection). Gordon Griffin, an associate in Crowell & Moring LLP's Government Contracts Group, works and speaks on a range of technology, cybersecurity, and privacy issues.

Corporate surveys have also underscored the pervasiveness of the economic espionage waged in cyberspace:

> Economic espionage, through cyber attacks committed by foreign intelligence services and other criminal enterprises is so pervasive that in a recent poll, 90 percent of companies admitted their networks had been breached in the past 12 months; while the other 10 percent could not say with certainty that they had not been penetrated.[7]

Similarly, a survey of 200 industry executives from the power, oil, gas, and water sectors indicated that "85 percent of respondents experienced network intrusions and that government-sponsored sabotage and espionage was the most often cited cyber threat."[8]

In summary, cyber espionage cuts across a broad spectrum of cutting-edge technologies and affects the overwhelming majority of major corporations and industrial sectors.

How Do Cyberspies Crack Digital Defenses?

Only the limits of imagination define the ways that cyberspies may break into networks to steal intellectual property or high-value secrets. Recently, the Russian gift bags handed out to world leaders at the G-20 summit contained USB thumb drives and three-pronged recharger cables bugged with Trojan horses to spy upon the leaders' communications.[9]

One of the classic cyber espionage techniques employs a five-step process (with some steps overlapping or moving in parallel): (1) establishing the foothold; (2) mapping the target network; (3) escalating the privileges; (4) entrenchment; and (5) exfiltration of data. These processes can take place over a period of years, with target companies or agencies completely unaware of the malicious presence on their networks.[10]

Establishing the Foothold

Often the penetration begins with a *spear-phishing attack* or *watering-hole exploitation*.[11] Once the target network had been compromised, the attacker will bypass the host network's firewall protection, instead establishing a connection that originates *inside* the host network.[12] The attacker then downloads more malware that both: (a) allows the espionage team to bypass authentication processes; and (b) facilitates later re-entry into the system.

Mapping the Network

Once cyberspies have established basic access to the network, reconnaissance proceeds. One of the famous cyber espionage groups (dubbed Advanced Persistent Threat—1 or APT1 by Mandiant) used batch scripts deploying system commands to return a text file with information on the network's configuration, accounts, and connections.[13] This technique opened a wide-angle picture into the nature of the compromised network, while also revealing the type of data housed inside the network.

Escalating Privileges

After reconnoitering the network, cyberspies then proceed with escalating privileges within the host network. Commonly, this step involves acquiring legitimate user credentials (user names and passwords) to impersonate authorized network users. On networks that have "hashed" their user's passwords, a number of publicly available software tools allow cyberspies to acquire the password hashes from the host network. In some instances, cyberspies can use a hashed password as is, bypassing the hash, or (if the attackers have sufficient computing resources) cracking the hash with brute force and determining the actual password.[14]

Entrenchment

Next, cyberspies work to ensure unfettered access to and a resilient presence on the network in the event that the victim discovers and deletes the initial backdoor. This entrenchment typically involves the installation of new backdoors in other corners of the network labyrinth and the use of web portals

and virtual private networks (VPNs) to bypass network security.[15] Virtual private networks and web portals both function on the same premise: they turn the attacker's computer into a "thin client" that in turn uses network resources for computing. Like a double agent, the cyberspy has effectively turned the victim's network into the attacker's own computer. In networks that only require single-factor authentication, stolen user credentials can allow a high degree of access through VPNs and web portals.

Exfiltration of Data

Once the cyberspies have mapped out a network and gained access to the coveted data and technology, the final step is a physical spy's equivalent of the handoff or dead-drop: bundling the data into manageable packets and exporting them outside of the host network to a location controlled by the attackers. Cyberspies can accomplish this by using an archiving utility, and then transferring the files using existing backdoors or file transfer protocols (FTPs).

What Are the Economic Impacts of Cybertheft?

The US economy runs on the rocket fuel of intellectual property, trade secrets, and innovative technologies—which account for $5.06 trillion of the domestic product.[16] Unfortunately, this same intellectual wealth attracts relentless cyberlooters. According to a public report of a classified National Intelligence Estimate (NIE), "the United States is the target of a massive, sustained cyber-espionage campaign that is threatening the country's economic competitiveness."[17]

As a result, cyber espionage has now escalated to "the greatest transfer of wealth in human history."[18] Although estimates vary, the cybertheft losses now tally to hundreds of billions of dollars:

> China's cyber espionage against U.S. commercial firms poses a significant threat to U.S. business interests and competitiveness in key industries. General Keith Alexander, Director of the National Security Agency and commander of U.S. Cyber Command, assessed that the financial value of these losses is about $338 billion a year, including intellectual property losses and the down-time to respond to penetrations, although not all those losses are [due] to Chinese activity.[19]

These macrocyberthreats and losses may not readily translate into a comprehensible business case for a chief executive officer (CEO), chief financial officer (CFO), or general counsel to take aggressive action to bolster cyberdefenses within an individual corporation, laboratory, or university. However, a compelling business case does exist. At the individual entity level, the cyberthreat is—in a word—catastrophic. The examples below illustrate the havoc that cyber espionage wreaks upon individual corporations and organizations.

Lost Terabytes

With skyrocketing cyberthefts, data losses for individual companies must often be measured in terabytes. According to Mandiant's report, the Chinese APT1 hackers have "systematically stolen hundreds of terabytes of data from at least 141 organizations," including one instance of "APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period."[20] In another instance, cyberspies "stole millions of pages of sensitive research documents" over several years from a robotics company—that then saw a competing robotics firm use its design in China.[21] Perhaps the most dramatic loss involved a single company losing 38 terabytes of data to a cyberpenetration:

> As an example of the scale of the threat, one American company had 38 terabytes of sensitive data and intellectual property exfiltrated from its computers—equivalent to nearly double the amount of text contained in the Library of Congress.[22]

Economic Losses

For individual corporations, the economic impact of cyberattacks and data theft may literally bet the company's future ability to compete in the global market.

For example, a 2011 FBI report noted, "a company was the victim of an intrusion and had lost 10 years' worth of research and development data—valued at $1 billion—virtually overnight."[23]

In another instance, Britain's head of the MI5 domestic security service stated that "digital intruders targeting a 'major London listed company' had caused a loss of 800 million pounds ($1.3 billion), in part because of the resulting disadvantage in 'contractual negotiations."[24] Another company nearly lost one-eighth of its profits when a departing employee unlawfully downloaded proprietary paint formulas valued at $20 million.[25]

Compromised Mergers and Negotiations

Increasingly, hackers have targeted high-value corporate mergers and negotiations, thus compromising highly sensitive data, putting corporate victims at serious disadvantage during negotiations, and even undermining the parties' ability to close deals.

- *$2.4 Billion M&A Deal.* "The PLA in 2009 may have conducted a 'spearphishing' campaign against the Coca-Cola Corporation. The alleged attack coincided with Coca-Cola's attempts to acquire China Huiyuan Juice Group for $2.4 billion, which would have been the largest foreign takeover of a Chinese company. Hackers gained access to sensitive corporate documents, presumably targeting Coca-Cola's negotiation strategy. Shortly after the FBI informed Coca-Cola that its network was compromised, the acquisition collapsed."[26]
- *$40 Billion M&A Deal.* "China-based cyberthieves, for instance, hacked into the computer networks of seven law firms in 2010 to get more information about

BHP Billiton Ltd.'s ultimately unsuccessful $40 billion bid to acquire Canadian company Potash Corp. of Saskatchewan, Inc., Bloomberg reported in January."[27]

- *Double-Digit Negotiation Loss*. "Over the following 2.5 years, APT1 stole an unknown number of files from the victim and repeatedly accessed the email accounts of several executives, including the CEO and General Counsel. During this same time period, major news organizations reported that China had successfully negotiated a double-digit decrease in the price per unit with the victim organization for one of its major commodities."[28]

In summary, these gargantuan losses of intellectual property, trade secrets, and technology pose some rather fundamental questions for that individual corporation.

- Will the company survive?
- If so, will the CEO, CFO, and General Counsel have jobs tomorrow?
- If so, what will they say to the regulators, investigators, shareholders, and media?

Standing alone, the losses—$1 billion in technology, a $2.4 billion business deal, or 38 terabytes of data—represent a body blow for nearly any company. But such losses may be only the first cycle of pain. The next cycle may commence with regulatory investigations, shareholder litigation, and/or onerous reporting obligations.

What Are the Legal Implications for Cybervictims?

In the recent past, silence often shrouded massive data breaches and intellectual property losses from cyber espionage.[29] However, escalating disclosure duties make silence an ever-more risky strategy. Three areas illustrate the legal risks of remaining mum after cyberspies execute digital heists of corporate secrets and technology.

SEC Cybersecurity Guidelines

In October 2011, the Securities and Exchange Commission (SEC) issued guidance for publicly traded companies to report on material risks relating to cybersecurity.[30] In this cybersecurity guidance, the SEC identified several key risk areas to be addressed by publicly traded companies.

- *Material Risks*. Due to cyberattacks, companies must weigh the risks relating to lost intellectual property, disrupted operations, security breach remediation, and reputational damage.
- *Cyberrisk Assessment*. The corporate risk assessments for cyberattacks should include the probability of cyberattacks, the quantitative and qualitative magnitude of such cyberrisks, and potential impact of costs and "other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."[31]
- *Adequacy of Cybersafeguards*. In making their cyberrisk assessment, companies should "consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware."[32]
- *Intellectual Property Losses*. The SEC guidelines expressly address corporate reporting duties for intellectual property losses: "For example, if 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."[33]

ONLY THE LIMITS OF IMAGINATION DEFINE THE WAYS THAT CYBERSPIES MAY BREAK INTO NETWORKS TO STEAL INTELLECTUAL PROPERTY OR HIGH-VALUE SECRETS.

DO YOU HAVE ANY TECHNOLOGY OR SECRETS WORTH STEALING? IF SO, YOU ARE PROBABLY AN ESPIONAGE TARGET.

Shareholder and Fiduciary Obligations

Increasingly, shareholders and business partners have significant concerns about how stout a corporation's cybersecurity defenses may be. Global Payments' stock fell more than nine percent before trading was halted[34] following a security breach unrelated to cyber espionage. Another company saw its stock plunge 90 percent after cyberspies stole its source code and began producing competing products.[35] Such losses of market value will expose companies to heightened litigation risks. In its landmark report on cyber espionage, the Office of the National Counterintelligence Executive emphasized the "Judicial Mandate for Boards of Directors to Secure Corporate Information," raising the specter of shareholder actions against the corporation and Board of Directors for intellectual property and trade secret losses stemming from inadequate cybersecurity defenses:

> Delaware's Court of Chancery ruled in the 1996 Caremark case that a director's good faith duty includes a duty to attempt to ensure that a corporate information and reporting system exists and that failure to do so may render a director liable for losses caused by the illegal conduct of employees. The Delaware Supreme Court clarified this language in the 2006 Stone v. Ritter case—deciding that directors may be liable for the damages resulting from legal violations committed by the employees of a corporation, if directors fail to implement a reporting system or controls or fail to monitor such systems.[36]

Military Technology

Multiple reports have warned that US defense contractors remain near the top of the list as targets for cyber espionage.[37] For example, the FBI described the theft of dual-use technology and military grade equipment "from unwitting U.S. companies" as "one of the most dangerous threats to national security."[38]

On November 13, 2013, the Department of Defense (DoD) issued regulations to counter this threat, mandating that defense contractors implement additional cybersecurity measures to protect "controlled technical information."[39] The regulations broadly define "technical information" to include "research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders," and more.[40] Among other requirements, this regulation requires contractors to:

- Report within 72 hours of discovery any "cyber incident" (defined as an action that results in an actual or potentially adverse impact on an information system and/or the information residing therein);
- Preserve relevant data for at least 90 days;
- Conduct an internal review of the contractor's network for evidence and extent of any compromise of data;
- Cooperate with DoD investigations for "damage assessments"; and
- Flow the clause down to subcontractors (even for commercial items).[41]

Conclusion

Like smashing atoms, the fusion of economic espionage and cybertheft techniques has fundamentally and irreversibly transformed the world: (1) cyber espionage now targets a virtually boundless list of innovations, technologies, and secrets; (2) the impact of a major cyberheist can be a virtual bet-the-company (or bet-your-career) event; and (3) silence about a major breach and loss of intellectual property or trade secrets may expose a company to serious sanctions and litigation, thus compounding the economic impact of the losses themselves. In the Age of Cyber Espionage, organizations now have even more powerful business cases for hardening cyberdefenses to protect the very technologies, innovations, and secrets upon which they have built their reputations and staked their futures. ◆

Endnotes

1. *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, The White House Office of the Press Secretary (May 29, 2009) (http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure).

2. *An Introduction by General Alexander*, The Next Wave, Vol. 19, No. 4 (2012) (http://www.nsa.gov/research/tnw/tnw194/article2.shtml).

3. Michael Riley & John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, Bloomberg.com (Dec. 14, 2011) (http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html).

4. ONCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, at 8–9 (Oct. 2011) (http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf) (hereinafter ONCIX Economic Espionage Report).

5. DSS, *Targeting U.S. Technologies,* at 9 (2013) (http://www.dss.mil/documents/ci/2013%20Unclass%20Targeting%20US%20Technologies_FINAL.pdf).

6. DNI, *Worldwide Threat Assessment of the US Intelligence Community,* at 2 (Mar. 12, 2013) presented to the Senate Select Committee on Intelligence (http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf).

7. *Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security: Hearings Before House Homeland Security Comm.,* 112th Cong. (June 28, 2012) (statement of Rep. Higgins) (hereinafter 2012 House Economic Espionage Hearings) (http://www.cq.com/doc/congressionaltranscripts-4116637?print=true).

8. *ONCIX Economic Espionage Report,* Annex B (Oct. 2011).

9. Carol Williams, *Kremlin Slips Spying Gadgets Into G20 Summit Gift Bags, Newspapers Say*, L.A. Times (Oct. 29, 2013) (http://articles.latimes.com/2013/oct/29/world/la-fg-wn-russia-g20-summit-gifts-spy-devices-20131029).

10. *See* Ryan Sherstobitoff, Itai Liba, and James Walter, *Dissecting Operation Troy: Cyberespionage in South Korea* (http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf); *see also Cyber Espionage and the Theft of U.S. Intellectual Property and Technology: Hearings before House Subcomm. on Oversight and Investigations of the Energy Comm.*, 113th Cong. (July 9, 2013) (statement of Larry M. Wortzel) (hereinafter 2013 House Cyber Espionage Hearings) (http://energycommerce.house.gov/hearing/cyber-espionage-and-theft-us-intellectual-property-and-technology).

11. Alex Cox, *The Cyber Espionage Blueprint: Understanding Commonalities in Targeted Malware Campaigns* (July 2013) (https://blogs.rsa.com/wp-content/uploads/2013/07/BLUEPRINT_WP_0713_final.pdf).

12. Verizon, *2013 Data Breach Investigations Report*, at 31 (http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf).

13. Mandiant Corp., *APT1: Exposing One of China's Cyber Espionage Units*, pp. 35–36 (Feb. 12, 2013) (http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) (hereinafter "Mandiant Report").

14. Kapersky Lab Global Research and Analysis Team, *The Icefog APT: A Tale of Cloak and Three Daggers* (http://www.securelist.com/en/downloads/vlpdfs/icefog.pdf).

15. Mandiant Report, pp. 36–37.

16. 2012 House Economic Espionage Hearings (statement of Mr. Graham, Chief Economist, U.S. Patent and Trademark Office).

17. Ellen Nakashima, *U.S. Said to Be Target of Massive Cyber-Espionage Campaign*, Wash. Post (Feb. 10, 2013).

18. *An Introduction by General Alexander*, The Next Wave, Vol. 19, No. 4 (2012) (http://www.nsa.gov/research/tnw/tnw194/article2.shtml).

19. 2013 House Cyber Espionage Hearings (statement of Larry Wortzel); *see also id.* (statement of James Lewis estimating losses at "1% of America's GDP"); McAfee and CSIS, *The Economic Impact of Cybercrime and Cyber Espionage*, at 16 (July 2013) (estimating cyber espionage and crime at between $70 billion to $140 billion).

20. Mandiant Report, at 3.

21. 2013 House Cyber Espionage Hearings (statement of Larry Wortzel).

22. Sen. Sheldon Whitehouse, *We Need to Act on Cybersecurity*, Natl. L.J. (May 10, 2010).

23. Congressional Research Service (CRS), *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, pp. 2–3 (Mar. 1, 2013) *quoting* Executive Assistant Director Shawn Henry, *Responding to the Cyber Threat*, FBI, Baltimore, MD, 2011.

24. Ben Elgin, Dune Lawrence & Michael Riley, *Coke Gets Hacked and Doesn't Tell Anyone*, Bloomberg.com (Nov. 4, 2012) (http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html).

25. *ONCIX Economic Espionage Report,* at 3.

26. 2013 House Cyber Espionage Hearings (statement of Larry Wortzel).

27. Ben Elgin, Dune Lawrence & Michael Riley, "*Coke Gets Hacked and Doesn't Tell Anyone*, Bloomberg.com (Nov. 4, 2012) (http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html).

28. Mandiant Report, at 25.

29. Ben Elgin, Dune Lawrence & Michael Riley, *Coke Gets Hacked and Doesn't Tell Anyone*, Bloomberg.com (Nov. 4, 2012) (http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html).

30. SEC, *Cybersecurity: CF Disclosure Guidance: Topic No. 2* (Oct. 13, 2011) (http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm).

31. *Id.,* at 3.

32. *Id.*

33. *Id.,* at 4.

34. GAO, *Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage,* at 7 (GAO-12-876T) (June 28, 2012) (http://www.gao.gov/products/GAO-12-876T).

35. 2013 House Cyber Espionage Hearings (statement of Rep. Murphy).

36. *ONCIX Economic Espionage Report,* Annex A, at A-2 to A-3.

37. *See, e.g.,* DSS, *Targeting U.S. Technologies,* at 9 (2013); *ONCIX Economic Espionage Report*, pp. 8–9.

38. 2012 House Economic Espionage Hearings (statement of Mr. Woods, Asst. Director, U.S. Immigration & Customs Enforcement, DHS).

39. 78 Fed. Reg. 69273, 69279 (2013), implementing Department of Defense Acquisition Regulation Supplement (DFARS) Subpart 204.73 *Safeguarding Unclassified Controlled Technical Information* (http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf).

40. *Id.*

41. *Id.,* at 69279–82.