The Insider Threat:

Why Chinese hacking may be the least of corporate worries

Kroll Advisory Solutions℠

Table of Contents

Introduction

On January 31, 2013, the New York Times announced that it was a victim of a Chinese hacking operation in which the intruders had been on the news organization's network for at least four months. A day later, the Wall Street Journal made a similar announcement. Papers nationwide carried the story with ominous warnings about the Chinese hacking menace and the threat it presented to U.S. businesses. Less than a month later, the cyber security company Mandiant released a report identifying a Chinese military unit as a major source for numerous hacks on U.S. business networks,[1] thus adding to the feverish reporting on the Chinese hacking threat.

In actuality, hacking of this type—where foreign hackers penetrate networks and stay there for long periods of time—is old news to the cyber security community. For a number of years, leading experts have warned of this type of hacking, often referred to as Advanced Persistent Threats ("APTs"). APTs use 0-day exploits or malware that has yet to be discovered by anti-virus vendors, thereby making their detection using conventional means extremely difficult.

Company insiders, not outside hackers, are involved in more than two-thirds of all cyber cases involving theft of intellectual property.

Corporate Insiders v. State-sponsored Hacking

Are APTs and other forms of hacking a serious threat to companies' trade secrets and proprietary data? No question. But are they the largest such threat that companies face? The answer remains "no." Company insiders, not outside hackers, are involved in more than two-thirds of all cyber cases involving theft of intellectual property.[2] Moreover, when there is intentional and malicious destruction of data, a corporate insider is frequently responsible. Whether driven by opportunism, greed, a desire for revenge, or a combination of all three, these insiders exploit their positions of trust to obtain access to their organization's most valued digital assets. Moles, opportunists, contractors, disgruntled employees, and ex-IT personnel—all currently pose a greater risk to corporate intellectual property than state-sponsored hacking and APTs, both in frequency and in damage caused. According to CSO Magazine's 2011 CyberSecurity Watch Survey:

> "Not only are insider attacks monetarily costly, but they also cause additional harm to organizations that can be difficult to quantify and recoup. Harm to an organization's reputation, critical system disruption and loss of confidential or proprietary information are the most adverse consequences from insider cybersecurity events, according to respondents. The public may not be aware of the number of insider events or the level of the damage caused because 70% of insider incidents are handled internally without legal action..."[3]

Statistics only go so far in describing the severity of risk caused by this particular type of cyber threat. Real-life examples paint a more complete and persuasive picture, and such examples abound in the record of federal prosecutions. The FBI doubled the number of trade secret arrests in the last four years,[4] and the overwhelming majority of those prosecutions involved insiders.[5]

Case #1 **Economic Espionage:** On December 21, 2011, in the U.S. District Court for the District of Indiana, defendant Kexue Huang was sentenced to seven years and three months' imprisonment after his conviction on charges of economic espionage and theft of trade secrets. The charges principally concerned the theft of trade secrets related to a commercial insecticide developed by Dow Chemical Co. in Indiana, where Huang, a Canadian national, worked as a research scientist from 2003 to 2008, when he was fired. He admitted to stealing $300 million worth of Dow trade secrets and delivering them to the People's Republic of China ("PRC") and Germany through an intermediary. He used the trade secrets to conduct unauthorized research with the intent to benefit foreign universities that were instrumentalities of the PRC government. Huang also admitted that after he was fired by Dow, he went to work as a biotechnologist for grain distributor Cargill. Again, while employed by Cargill, he stole a trade secret involving a key component of a new Cargill food product, which he then gave to a student at Hunan Normal University in China. If there is such a thing as a serial malicious insider, Huang fits the bill.

If there is such a thing as a serial malicious insider, Huang fits the bill.

At the time of Huang's guilty plea, the head of the FBI's field office in Indiana stated:

> "Among the various economic espionage and theft of trade secret cases that the FBI has investigated in Indiana, the vast majority involve an inside employee with legitimate access who is stealing in order to benefit another organization or country. This type of threat, which the FBI refers to as the Insider Threat, often causes the most damage."[6]

Case #2 **The Opportunist:** On August 29, 2012, Hanjuan Jin was sentenced to four years' imprisonment for stealing Motorola trade secrets. She had been a software engineer at Motorola from 1998 through February 2007. While on medical leave in 2006, Jin accepted employment with a Chinese competitor company, Sun Kaisens. She then returned to work at Motorola. At various times from February 26-27, 2007, Jin downloaded from Motorola's secure internal computer network numerous proprietary technical documents and removed several documents and other materials from the company's offices. Also on February 27, Jin e-mailed her manager to give notice that she would be leaving Motorola immediately. The following day, she was arrested at Chicago's O'Hare Airport after purchasing a one-way ticket to China. Police found her in possession of more than 1,000 electronic and paper documents belonging to Motorola.

Case #3 **The Mole:** In February 2010, Greg Chung, a former Rockwell and Boeing engineer, was sentenced to more than 15 years' imprisonment for acting as an agent of the PRC and stealing trade secrets about the Space Shuttle, the Delta IV rocket, and the C-17 military cargo jet for the benefit of the Chinese government. In a September 2006 search of Chung's residence, FBI and NASA agents found more than 250,000 pages of documents from Boeing, Rockwell, and other defense contractors inside the house and in a crawl space underneath the house. Among the documents were scores of binders containing decades' worth of stress analysis reports, test results, and design information for the Space Shuttle. Chung also sent numerous engineering manuals to the PRC, including 24 manuals relating to the B-1 bomber that Rockwell had prohibited from disclosure outside the company and select federal agencies.

Before leaving, he downloaded numerous computer files...

Case #4 **The Disgruntled Ex-Employee:** In March 2010, Michael Mitchell was sentenced to 18 months in prison and ordered to pay his former employer more than $187,000. Mitchell had soured on his job at DuPont as a Kevlar® marketing executive, and ultimately he was fired for poor performance. Before leaving, he downloaded numerous computer files with DuPont trade secrets and gave them to Kolon Industries, a South Korean competitor of DuPont's Kevlar products with which Mitchell entered into a consultant agreement. In this case, however, there may yet be a happy ending for the victim—or, at least, a not-so-unhappy ending. On September 14, 2011, a jury in the U.S. District Court for the Eastern District of Virginia awarded DuPont damages in the amount of $919.9 million.[7] That civil judgment is on appeal. On October 18, 2012, the U.S. Department of Justice indicted Kolon Industries and several of its executives and employees for engaging in a multi-year campaign to steal trade secrets related to DuPont's Kevlar products.[8] The indictment seeks forfeiture of at least $225 million in illicit proceeds.

Case #5 **The Disgruntled Systems Administrator:** In December 2012, Switzerland's intelligence service (the NDB) informed their U.S. and British counterparts of a major data theft by an NDB IT administrator involving terabytes of sensitive and classified data.[9] The IT technician, an 8-year employee with administrative rights to most of the NDB network, became disgruntled at his job because NDB management failed to implement his suggestions for improved systems management. He reportedly used his authorized access to copy huge amounts of intelligence data onto small portable drives, which he then smuggled outside in his backpack. He is believed to have tried to sell the data to third parties before he was arrested. The stolen material included classified data from both the British (MI6) and U.S. (CIA) intelligence services.

Reducing the Risk from Insider Cyber Threat

The news is not all bad. A 2012 insider threat study by Carnegie Mellon University's Software Engineering Institute[10] examined fraud and illicit cyber activity in the U.S. financial services sector. Among other findings, the study concluded that (1) an average of 32 months elapsed between the beginning of the fraud and its detection by the victim organization, and (2) the insiders' means were not especially sophisticated. These findings suggest both that companies are not particularly good at monitoring illicit cyber activity within their own networks, and that this deficiency is not due to the cyber skills of the malicious insiders. Thus, there is reason for optimism: If the insider cyber threat receives appropriate priority within an organization's security and compliance hierarchy, there appears to be ample room for improved detection and prevention.

What steps can companies take to reduce the risk of insider cybercrime?

More practically speaking, what steps can companies take to reduce the risk of insider cybercrime? For a start, they can get better at profiling those employees most likely to commit such crimes. According to CSO Magazine's 2012 CyberSecurity Watch Survey,[11] organizations that experienced cybercrime by an insider in the previous 12 months reported that 51 percent of those insiders violated IT security policies and 19 percent were flagged by a manager for behavior/performance issues. Thus, closer monitoring of employees exhibiting either of these two characteristics might help companies prevent or more quickly detect up to 70 percent of insider cybercrimes.

The FBI's website provides a longer list of at-risk behavioral traits, including unreported foreign trips, seeking proprietary or classified information unrelated to work duties, paranoia about being investigated, and disproportionate anger over career disappointments.[12] And when an employee leaves an organization, voluntarily or involuntarily, strict termination procedures should be in place to ensure that all network access privileges are terminated immediately. While that may seem self-evident, it is remarkable how often it is overlooked or addressed too late.

Detection and prevention efforts should not rely solely on monitoring at-risk employees. Companies also need effective, internal monitoring of their networks so as to better identify unusual or suspicious user patterns when they occur. To that end, among other measures, IT security should use centralized, system-wide logging to track data access and transference generally, and implement strict access controls for all files and data centers containing trade secrets or other sensitive or proprietary data. Such logging is important not only to real-time monitoring, but also to historical investigations after an incident occurred.

Without the digital footprints provided by network logs, it can be virtually impossible for even the most skilled forensics investigator to reconstruct what happened and identify the real cause. Thus, log retention policies should ensure accessibility for a meaningful length of time (e.g., one month of logs immediately accessible and two years archived). And finally, all network logging devices should be configured to transmit to a centralized, secure location where the logs can be preserved, backed up, and securely archived. This makes an investigator's job much easier. Rather than collecting logs from hundreds of network devices in different locations on a network, an investigator can instead go to one location where all the key data is collected and securely maintained.

This list of security suggestions is hardly exhaustive, and its intent is simply to provide a bit of practical advice for companies on how to minimize risk from malicious insiders. While hacking crimes involving China and other nations will continue to receive national press coverage, organizations should not lose sight of the fact that insiders, not outside hackers, still pose the greatest risk for theft of intellectual property and other proprietary data on their networks.

About the author

Michael DuBose
Managing Director
Cyber Investigations Practice Leader

Michael DuBose is a Managing Director and Cyber Investigations Practice Leader for Kroll Advisory Solutions. Michael and the Cyber Investigations team provide comprehensive investigative services for digital forensics, data breach response, and complex cybercrimes. Prior to joining Kroll Advisory, Michael served as Chief of the Computer Crime and Intellectual Property Section (CCIPS) at the United States Department of Justice (DOJ), where he supervised 40 federal prosecutors and managed some of the largest investigations and prosecutions ever brought in the U.S. involving computer network intrusions, international phishing schemes, botnets, hacktivist groups, copyright piracy, theft of trade secrets, and large-scale data breaches—including the prosecution of hacker Albert Gonzalez for stealing more than 130 million credit and debit card numbers from TJX, Hannaford, Heartland Payment Systems, and others. Michael previously was Senior Counsel for Enforcement at the U.S. Department of Treasury, and also served for more than seven years as an Assistant U.S. Attorney in the District of Maine. He is a two-time winner of the Department of Justice Director's Award, a three-time winner of Assistant Attorney General Awards for combating online crime and copyright piracy, and in 2011 he received the Criminal Division's highest award—the Henry E. Peterson Memorial Award.

Notes

1 http://www.cnn.com/2013/02/19/business/china-cyber-attack-mandiant/

2 http://www.darkreading.com/taxonomy/index/printarticle/id/240144559

3 The 2011 CyberSecurity Watch Survey (January 2011): CSO Magazine in cooperation with the Software Engineering Institute CERT Program at Carnegie Mellon University, the U.S. Secret Service, and Deloitte.

4 http://www.fbi.gov/news/testimony/economic-espionage-a-foreign-intelligence-threat-to-americans-jobs-and-homeland-security

5 For examples of economic espionage and trade secret prosecutions involving insiders, see:

18 U.S.C. §1831 – Economic espionage

- (http://www.justice.gov/usao/can/news/2012/2012_03_02_chao.guiltyplea.press.html)
- (http://www.justice.gov/opa/pr/2012/February/12-nsd-180.html)
- (http://www.justice.gov/opa/pr/2011/December/11-crm-1696.html)
- (http://www.justice.gov/usao/ma/news/2011/August/DoxerElliotPleaHearingPR.html)
- (http://www.justice.gov/criminal/cybercrime/press-releases/2009/chungConvic.pdf)
- (http://www.justice.gov/usao/iln/pr/chicago/2012/pr0829_01.pdf)

18 U.S.C. §1832 – Theft of trade secrets

- (http://www.justice.gov/usao/mie/news/2012/2012_11_30_sdu.html) (http://www.justice.gov/usao/kyw/news/2012/20121015-01.html)
- (http://www.justice.gov/usao/vae/news/2012/10/20121018kolonnr.html)
- (http://www.justice.gov/usao/can/news/2012/2012_05_09_zhang.convicted.press.html)
- (http://www.justice.gov/usao/txs/1News/Releases/2012%20April/120427%20Huang.html)
- (http://www.justice.gov/opa/pr/2012/January/12-crm-051.html)
- (http://www.justice.gov/usao/nys/pressreleases/July06/yuchangshengpleapr.pdf)
- (http://www.fbi.gov/albany/press-releases/2011/former-bristol-myers-employee-sentenced)
- (http://www.justice.gov/criminal/cybercrime/press-releases/2011/samarthSent.pdf)
- (http://www.justice.gov/criminal/cybercrime/press-releases/2011/linSent2.pdf)
- (http://www.justice.gov/usao/iln/pr/chicago/2010/pr1208_01.pdf)
- (http://www.justice.gov/criminal/cybercrime/press-releases/2010/crowSent.pdf)
- (http://www.justice.gov/criminal/cybercrime/press-releases/2010/howleyPlea.pdf)
- (http://www.justice.gov/criminal/cybercrime/press-releases/2010/zhangArrest.pdf)
- (http://www.justice.gov/criminal/cybercrime/press-releases/2008/mengSent.pdf)

6 http://www.justice.gov/opa/pr/2011/October/11-crm-1372.html (Special Agent in Charge Roger Holley)

7 http://www.bbc.co.uk/news/business-14925058

8 http://www.examiner.com/article/dupont-vs-kolon-fight-results-indictments-of-top-executives

9 http://www.americanthinker.com/blog/2012/12/swiss_spy_agency_suffers_massive_counterterrorism_data_leak.html; http://www.theregister.co.uk/2012/12/04/swiss_intelligence_data_loss/

10 Cummings, Adam; Lewellen, Todd; McIntire, David; Moore, Andrew; and Trzeciak, Randall. Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector (CMU/SEI-2012-SR-004). Software Engineering Institute, Carnegie Mellon University, 2012. http://www.sei.cmu.edu/library/abstracts/reports/12sr004.cfm

11 The 2012 CyberSecurity Watch Survey (April 2012): CSO Magazine in cooperation with the Software Engineering Institute CERT Program at Carnegie Mellon University, the U.S. Secret Service, and Deloitte).

12 http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

Contact Us

For more information, call or visit us online
866.419.2052 | www.krollcybersecurity.com
www.krolladvisory.com

Kroll Advisory Solutions℠