Connecticut Law Tribune
MARCH 14, 2011
VOL. 37, NO. 11 • $10.00
An ALM Publication
CTLAWTRIBUNE.COM

Businesses Must Protect Against Cyber-Espionage

Attacks by employees or hackers can lead to civil, criminal charges

By T. SCOTT COWPERTHWAIT

The 2010 science fiction thriller "Inception" tells the story of a corporate spy and saboteur who is hired to invade the dream state of the heir to an energy empire. His mission is to plant a "new idea" inside the heir's mind, thus altering the future of the business.

While the concept of entering the human mind through dreams for espionage purposes seems far-fetched, similarities exist with respect to cyber-related economic espionage threats and vulnerabilities to businesses. Even an unsophisticated malware attack launched against a corporate computer network can cause significant economic damage, decrease competitive advantage, devalue brand recognition and reputation and undermine consumer confidence in the targeted business or industry.

Targeted Industries

The rapidly changing and increasingly complex tools and capabilities used to infiltrate corporate computer networks and access proprietary corporate information and systems present new challenges to businesses. For companies in the private sector, the theft of trade secrets, critical technologies and other proprietary and sensitive business information can have serious effects on information technology, security, human resources and business planning which can lead to civil, criminal and/or regulatory actions or charges.

While a major corporation may be capable of withstanding the damage caused by economic espionage, small and mid-sized businesses whose value is typically tied to a single piece of technology or trade secret are less likely to survive. These businesses generally have limited resources or pay little to no attention to developing an effective cybersecurity program and, therefore, the damage resulting from economic espionage can be catastrophic.

Recent cases demonstrate that both criminal and civil enforcement of economic and industrial espionage for theft of trade secrets, proprietary and sensitive information and disruption of critical infrastructure is proceeding at an accelerated pace among the private sector and the U.S. government.

The most likely criminal charges are filed pursuant to statutes that include: 1) Economic Espionage Act; 2) Computer Fraud and Abuse Act; 3) Arms Export Control Act; 4) foreign/interstate transportation of stolen property; 5) mail and/or wire fraud; 6) honest services fraud; 7) money laundering; 8) false statements; and 9) obstruction of justice.

The most common perpetrator remains the corporate insider. A current or recently terminated employee does not need to launch sophisticated computer intrusions because he or she likely has knowledge of and/or access to the targeted computer network or data. For example, in February 2010, a grand jury sitting in the U.S. District Court for the Southern District of New York returned an indictment charging Sergey Aleynikov, a computer programmer employed by Goldman Sachs, with theft of trade secrets in violation of the Economic Espionage Act, transportation of stolen property in interstate and foreign commerce, and unauthorized computer access in violation of the Computer Fraud and Abuse Act. After accepting an employment offer with Teza Technologies LLC, a startup company dedicated to developing its own high-frequency trading business, Aleynikov had uploaded, compressed and encrypted hundreds of thousands of lines of source code, proprietary data housed on Goldman Sachs's servers, and transferred the data to an external server for future retrieval. While the court dismissed the count pursuant to the Computer Fraud and Abuse Act prior to trial, this past December the jury returned a guilty verdict on the remaining counts.


T. Scott Cowperthwait

In another case, also in December, the Hilton Hotel Corp. reportedly agreed to pay Starwood Hotels & Resorts $75 million in connection with Starwood's claims that Hilton officials, who were former Starwood

T. Scott Cowperthwait is a member of Pullman & Comley's Litigation Department and Cybersecurity and Infrastructure Protection Practice.

executives, stole confidential and proprietary information regarding Starwood's luxury, boutique hotel chain. Prior to the settlement, the U.S. Attorney's Office for the Southern District of New York moved to intervene and stay discovery in the civil action, raising the possibility that criminal charges pursuant to the Economic Espionage Act may be filed in connection with the corporate espionage acts.

Growing External Threat

But the corporate insider is not the only culprit with which companies should be concerned. There are more and more instances of both domestic and international espionage perpetrated by outsiders engaging in increasingly sophisticated tactics.

An emerging trend places criminal groups, hackers and, perhaps most alarmingly, nation-states at the epicenter of the economic and industrial espionage threat. While criminal groups and hackers tend to attack corporate computer networks for monetary gain or disruptive purposes, nation-states are sponsoring and/or engaging the services of these actors to launch cyber attacks against businesses to facilitate their information-gathering and espionage activities.

For example, last month, McAfee, a global security technology company, released a report finding that "coordinated covert and targeted cyber attacks have been conducted against global oil, energy, and petrochemical companies." These "Night Dragon" attacks, which originated from a server in China, are designed to steal specific, sensitive information, data and intellectual property by, among other things, penetrating computer networks through traditionally ordinary means (*e.g.,* an infected e-mail that appears to come from a legitimate business or contact).

Proactive Steps

Recent cyber attacks and other espionage-related acts on corporations highlight the threats posed by the connectivity of our computer networks and vulnerabilities of our proprietary and sensitive information. Businesses can take proactive steps to prepare for and protect against these potential threats and their possible legal (and business) repercussions by encouraging: 1) strong internal communication and coordination among essential parties, *e.g.*, physical and IT security, human resources, legal, management 2) identification of trade secrets and proprietary information/data, including non-traditional information, and analysis of potential loss (economic, reputation, competitive advantage, etc.) 3) identification of potential internal or external threats, corporate-wide awareness training and development of loss mitigation and prevention plans 4) development, implementation and enforcement of electronic and social media/networking use policies and 5) coordinated and effective relationships with law enforcement authorities.

Because the private sector owns most of the nation's critical infrastructure, it is likely that most economic and industrial espionage cases involving the theft or misappropriation of trade secrets and/or proprietary data will continue to be most effectively redressed through civil remedies. There is an increasing trend to pursue criminal remedies, although this approach relies heavily on a business's willingness to work with government investigators. Businesses, however, need to keep in mind that they themselves may be liable to government regulators and/or their investors for failing to properly secure against and/or disclose material events and acts, perhaps even attempted acts, of economic and industrial espionage. ■