BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Cybersecurity–It's Not Just About "National Security" Anymore: "Directors Desk" and Other Incidents Sound Wake-Up Call for the Executive Suite and Board Room

BY ALAN CHARLES RAUL

Media attention on the recent security incident disclosed by NASDAQ in connection with its "Directors Desk" application has focused attention on the potential for organized cybercriminals to access sensitive corporate documents, such as communications related to board of director meetings. But while the media, the government and the techie crowd may be up to speed on cybersecurity threats to trade secrets and other commercially sensitive information, corporate executives and directors may benefit from some information on the subject.

Alan Charles Raul is lead Global Coordinator for the Privacy, Data Security and Information Law practice of Sidley Austin LLP. He previously served as Vice Chairman of the White House Privacy and Civil Liberties Oversight Board, and as General Counsel of the Office of Management and Budget, among other government positions.

In 2010, the Director of National Intelligence called a self-disclosed intrusion into Google's network a national "wake-up call" demonstrating the need to get serious about cybersecurity. The rapid global dissemination of the "Stuxnet" worm—believed to target certain commercial equipment controlling uranium enrichment centrifuges—also reveals how pervasive computer vulnerability can be.

Even more recently, according to cybersecurity firm McAfee, hackers McAfee believed to be in China appear to have exfiltrated sensitive information from several international oil and energy companies for perhaps as long as four years. McAfee reported that the "coordinated covert and targeted cyberattack" victims included companies in the United States, Taiwan, Greece and Kazakhstan.

In addition, companies face "insider threats" from Wikileaks-type situations where sensitive data can be misappropriated and divulged by disaffected employees. Recent press reports suggest that various companies are currently subject to embarrassing and damaging disclosures from documents obtained by Wikileaks, from disgruntled insiders, or concerted hacking.

These recent incidents, and the striking *Foreign Affairs* article by the Deputy Secretary of Defense, and the very recent testimony of the Director of National Intelligence, provide a clear corporate lesson about corporate data security vulnerabilities. This issue extends well beyond protecting the personal or financial information of customers and employees. Valuable corporate information assets are exposed to at least as much risk. A few years back, businesses were primarily concerned about data breaches involving the personal information of consumers or employees, and the resulting

remediation costs and reputational injury. Now, businesses need to worry about core intellectual property assets being lifted from their servers, and directors should be asking whether trade secrets and other crucial information assets are adequately protected.

Business leaders need to ensure the protection of their companies' cyber-resources, along with attention to the corresponding legal issues and business imperatives. The threat has grown quickly. If your company is behind the curve, this must become a top-priority issue of corporate governance and internal controls, and not just a technical IT matter.

At a recent conference in Washington, Philip Reitinger, the deputy under secretary for the National Protection and Programs Directorate (NPPD), appealed to corporate CEOs and CFOs to meet with him and other government officials to better understand the profound dangers of and possible countermeasures to combat risks in cyberspace. Similarly, the Deputy Secretary of Defense and the Director of National Intelligence have stressed the need for the government to reach out to the private sector to collaborate more effectively on cybersecurity—not just out of a desire to be good corporate citizens, but because cybercriminals are targeting and stealing vast amounts of commercial information which could threaten the profitability and competitiveness of U.S. companies.

Characterizing cybersecurity as an urgent matter of ''national security'' may actually undermine getting the message across to the private sector. It is an urgent matter of corporate security and competitiveness. The fact is that corporations and executives have a crucial business imperative to take their responsibilities for cybersecurity far more seriously.

This summarizes a number of cybersecurity developments and issues, and provides a number of high-level recommendations for possible consideration by senior corporate management. Public companies should also consider the extent to which network intrusions and other cyber contingencies or risk factors merit disclosure in Securities and Exchange Commission filings.

The Magnitude of the Cyberthreat

Writing in the September/October 2010 issue of *Foreign Affairs* magazine, Deputy Secretary of Defense William J. Lynn discussed what he characterized as the most significant breach of U.S. military computers ever, and it served as an important wake-up call.''

This incident involved malicious computer code on a flash drive that uploaded itself onto a network run by the U.S. Central Command. Deputy Secretary Lynn revealed that the ''code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.''

Deputy Secretary Lynn stressed the vulnerability and critical role of the private sector. He warned that:

> Adversaries have acquired thousands of files from U.S. networks and from the networks of U.S. allies and industry partners, including weapons blueprints, operational plans, and surveillance data. . . . **Cyberthreats to U.S. national security are not limited to military targets.** Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks that control critical civilian infrastructure. Computer-induced failures of U.S. power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption. . . .
>
> Modern information technology also increases **the risk of industrial espionage and the theft of commercial information.** Earlier this year, Google disclosed that it had lost intellectual property as a result of a sophisticated operation perpetrated against its corporate infrastructure, an operation that also targeted dozens of other companies. **Although the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term.** . . .
>
> Computer networks themselves are not the only vulnerability. Software and hardware are at risk of being tampered with even before they are linked together in an operational system. Rogue code, including so-called logic bombs, which cause sudden malfunctions, can be inserted into software as it is being developed. As for hardware, remotely operated 'kill switches' and hidden 'backdoors' can be written into the computer chips used by the military, allowing outside actors to manipulate the systems from afar. **The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat.** Tampering is almost impossible to detect and even harder to eradicate.

In recent oral testimony before Congress Feb. 10, Director of National Intelligence (DNI) James Clapper also identified cyber-attacks as one of the leading threats to the country, not only to national security, but also to significant business interests. He said, ''we're also extremely focused on cyberthreats, as you are, and their impacts on our national security and economic prosperity. This threat is increasing in scope and scale, and its impact is difficult to overstate. . . . Additionally, we're seeing a rise in intellectual property theft. Industry has estimated that the loss of intellectual property worldwide to cyber crime in 2008 alone cost businesses approximate $1 trillion.''

In his written submission to Congress, DNI Clapper sounded the alarm for private industry even louder, and specifically noted the vulnerability of a company's ''crown jewels'' to cyber-risks. He noted that ''[l]ast year some of our largest information technology and defense contractor companies discovered that throughout much of 2009 they had been the targets of a systematic effort to penetrate their networks and acquire proprietary information. The intrusions attempted to gain access to and potentially modify the contents of source code repositories, the intellectual ''crown jewels of most of these companies.''

Cybersecurity Also a ''Tier One'' Risk for Companies Outside the United States

The threat is also not, of course, limited to major corporations in the United States. In a report issued on behalf of the Cabinet Office of the United Kingdom on Feb. 17, 2011, the United Kingdom stated that ''cyber threats are recognised by the Government as one of four 'Tier One' risks to the UK's security,'' and that despite what it ''believe[s] to be a significant under-

  PVLR ISSN 1538-3423

reporting of cyber crime,'' it ''is a national-scale issue'' whose ''cost to the economy . . . is significant and likely to be growing.'' The results of the U.K. report challenged the conventional wisdom that cyber crime is solely a matter of concern for government agencies and critical infrastructure industries. The U.K. report concluded that ''much larger swathes of industry are at risk [and] suggest[ed] that businesses need to look again at their defences to determine whether their information is indeed well protected.''

The U.K. report indicates that cyber-criminals range from foreign intelligence services and large organized crime groups, to disreputable (but otherwise legitimate) companies and individuals or small groups of opportunists. These groups engage in industrial espionage and IP theft that targets financial services, pharmaceutical and biotechnology companies, and software, electronics and high technology sectors.

Corporate Cyber-Attacks Pose Risks Distinct from Consumer Data Breaches

Everyone is well aware of the rash of data breach notification letters concerning consumer information that was potentially compromised, for example, through lost or stolen laptops and storage devices. Knowledge of this epidemic is primarily a reporting phenomenon; it results from notification statutes enacted by nearly all 50 states (and the federal government for banking, medical and certain telephone data). No comparable set of requirements exists outside of the consumer or personal context. Accordingly, awareness is considerably less acute regarding the exposure of corporate networks, computer resources and databases to large-scale criminal exploitation, but there is little reason to suspect that cybercriminals limit their interest to identity theft.

The risks to companies arise from highly sophisticated computer criminals that may or may not be actively supported by foreign governments. In addition to immediate financial windfalls, foreign intruders may be looking for longer term commercial advantages and opportunities to steal intellectual property (IP). Businesses involved in defense, national security or critical infrastructure sectors of the economy are particularly subject to the further risks that their computer resources could be targeted by foreign powers for geopolitical reasons or to support state-sponsored companies in non-capitalist countries.

Companies should, in particular, be aware of so-called ''advanced persistent threat'' (APT) in which intruders stealthily penetrate a network and create the ability over time to move throughout the system without detection and, sometimes nearly at will. Significantly, the APT intruder attempts to remain undetected for extended periods so that information can be tracked and leaked continuously, avoiding signatures and telltale signs of dramatic data losses. Numerous companies have suffered APT intrusions that have resulted in significant amounts of corporate intellectual property being exfiltrated to unknown destinations.

Government-Corporate Cooperation on Solutions

On Feb. 16, in a speech to a major cybersecurity conference in San Francisco (as reported by Washington Internet Daily), Mike McConnell, the same former DNI who labeled the Google hacking incident a national ''wake-up call'' on national security said, ''The odds are we'll wait for a catastrophic event'' for the U.S. government to impose cybersecurity requirements.'' McConnell noted that legislation could give legal protections for measures to protect networks as well as imposing liability for lapses. But former DNI McConnell said that when he was in office he ''didn't make the dent'' he had hoped for to advance sharing of information between the government and the private sector.

DHS Deputy Undersecretary Phil Reitinger echoed the information-sharing point at a Bisnow Media event co-sponsored by Sidley Austin LLP in Washington Feb. 18. Reitinger said the government must do better in collaborating with the private sector. ''We . . . have to recognize the risk and actually have a robust public dialogue about what we want the government to do, what we want the private sector to do, and how to create a framework so they all work together.'' But Reitinger commented that, ''Right now securing yourself is just too hard.''

At the San Francisco conference, a former Secretary of Homeland Security said that corporate directors would pay attention to a requirement for public companies to certify system risks, backups and resiliency, and a speaker from the Center for Strategic and International Studies said that the Sarbanes-Oxley Act ''was the one thing that worked'' in promoting the need for greater attention cybersecurity.

At the Bisnow/Sidley conference in Washington, the General Counsels of DHS (Ivan Fong) and the Commerce Department (Cameron Kerry), acknowledged that concerns over legal liability could inhibit companies from disclosing cyber-attacks and working with the government—and each other—in avoiding and mitigating cyber-risks. They suggested that new legislation from Congress could address these impediments and help overcome the private sector's reluctance to engage in greater collaboration on cybersecurity.

Public Disclosure Considerations

No current SEC disclosure requirements pertain to potential cyber-attacks. Nevertheless, some corporations have begun to include cybersecurity in their ''risk factors'' disclosures as well as provide notice of particularly significant network intrusions. Of course, if there has been a cyberattack that has material implications for securities holders, a corporation may be required to make disclosure under generalized disclosure requirements. Corporate boards are giving enhanced oversight to risk management and are typically including all aspects of information technology as a part of that process. Documents generated to provide directors with greater understanding of cybersecurity may also be relevant to the public disclosure posture of the corporation.

SEC filings have included disclosures such as this language:

> We regularly face attempts by others to gain unauthorized access through the Internet to our information technology systems by, for example, masquerading as authorized users or surreptitious introduction of software. These attempts, which might be the result of industrial or other espionage, or actions by hackers seeking to harm the company, its products, or end users, are sometimes successful. One recent and sophisticated incident occurred in January 2010 around the same time as the recently publicized security incident reported by Google. We seek to detect

and investigate these security incidents and to prevent their recurrence, but in some cases we might be unaware of an incident or its magnitude and effects. The theft and/or unauthorized use or publication of our trade secrets and other confidential business information as a result of such an incident could adversely affect our competitive position and reduce marketplace acceptance of our products; the value of our investment in R&D, product development, and marketing could be reduced; and third parties might assert against us or our customers claims related to resulting losses of confidential or proprietary information or end-user data and/or system reliability. Our business could be subject to significant disruption, and we could suffer monetary and other losses, including the cost of product recalls and returns and reputational harm, in the event of such incidents and claims.

* * *

Like many other government contractors, the Company's computer networks are subject to persistent intrusion attempts. The Company employs increasingly sophisticated technologies, operations and employee training in order to thwart such intrusions, but expects this to be a continuing challenge for the industry. When an intrusion is suspected, the Company takes prompt remedial steps and works closely with government authorities and customers to mitigate any adverse impacts. Based on a recent network intrusion, the Company is notifying customers it believes might have been affected and is working to address customer concerns. These efforts are ongoing and contractual exposure, if any, is not estimable at this time.

In 2009, a company was sued by shareholders for allegedly failing to disclose that it had been hit by a cyberattack. The disclosure was eventually linked to very significant data breach, and prompted a precipitous decline in the company's market value when the full extent of the attack was made public. The shareholders did not ultimately prevail in their securities lawsuit (8 PVLR 1758, 12/14/09). Thompson, U.S. District Judge for the District of New Jersey, rejected the securities fraud claims because ''Plaintiffs have not alleged facts sufficient to support an inference that Defendants knew that [the company] was not paying proper attention to its security problems.''

Going forward, however, companies would be well advised to ensure they ''pay proper attention to . . . security problems.''

Impediments to Individual Companies Addressing Cybersecurity

Because most of the nation's critical assets—including computer and information resources—are in private hands, cybersecurity cannot be addressed by the government alone. Companies, however, are understandably reluctant to publicize their vulnerabilities to serve the greater good, or to report problems to the government for the purpose of obtaining assistance or necessary information. Voluntary disclosure to federal agencies or law enforcement may trigger additional investigations, obligations and legal risks. Companies working together to combat cyber-attacks also present challenging competitive and perhaps antitrust issues.

Government Assistance on Cybersecurity

The government recognizes it must be more proactive in coordinating and facilitating the ability of the private sector to protect itself. The White House, Department of Homeland Security and Commerce Department (especially the National Institute for Standards of Technology) all have leadership roles in developing and implementing the national strategy for cybersecurity and protecting U.S. cyberspace.

Each sector of the economy involved in critical infrastructure industries (e.g., financial, transportation, utilities, etc.) has a joint government-corporate committee known as an ''information sharing and analysis center'' (ISAC). These ISACs were established pursuant to a Presidential Homeland Security Directive that mandates the public and private sectors to share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.

In addition, under the Federal Information Security Management Act, the Defense Department and Office of Management and Budget address expectations for information assets held by government contractors. While the National Security Agency has recently been designated the home for the military's ''Cybercommand,'' which leads development of offensive capabilities, the NSA also works with the Department of Homeland Security to provide guidance on certain issues for the private sector.

Government contractors obviously need to pay especially careful attention to the security and safeguards of government-related information assets.

Recommendations for C-Level Cybersecurity

As the ''Directors Desk'' and other incidents demonstrate, corporate networks and information assets are exposed at numerous points, and must thus be comprehensively safeguarded as part of an Information Governance strategy. For most larger companies, the Chief Executive and Board of Directors must take on cybersecurity as a significant matter of corporate governance. The context may be ''information technology,'' but the risks for the company could be existential or at least ''material.''

Accordingly, we recommend consideration of some or all of the following steps:

— As part of overall board oversight of risk management, CEOs report regularly to the Boards on their companies' cybersecurity risk profile and corresponding internal information governance systems. Companies should consider whether to include cybersecurity in their risk factor disclosures.

— Companies should develop, approve and implement a cybersecurity strategy under the direct supervision of a C-Level officer.

— Companies should consider how their trade secret and IP protection systems can be better secured in light of the manifest foreign and competitive threats.

— Companies should evaluate their ''insider threat'' risks, and adopt mitigation strategies to abate the damage that could be caused by Wikileaks-type situations.

— Employee training and awareness are critical to preventing, detecting and abating the risks of cyberattacks.

— Companies should prepare contingency and response plans for inevitable cybersecurity incidents.

  PVLR ISSN 1538-3423

— Companies should determine what government resources are relevant and available to assist internal efforts, and execute a strategy for taking advantage of the government's help before intrusions occur.

— Companies should review their particular legal and contractual environments to determine if they are subject to any special cybersecurity reporting or safeguard requirements

— Companies should aggressively monitor technological, industry and public policy developments on cybersecurity risks and remedies.