AUG/SEPT 2012 VOLUME 9/NUMBER 4 EXECUTIVECOUNSEL.INFO

ExecutiveCOUNSEL

THE MAGAZINE FOR THE GENERAL COUNSEL, CEO & CFO

NEW THREATS, NEW LEGAL DEVELOPMENTS, IN CYBERSECURITY

By Jamie Gorelick and Jonathan Cedarbaum

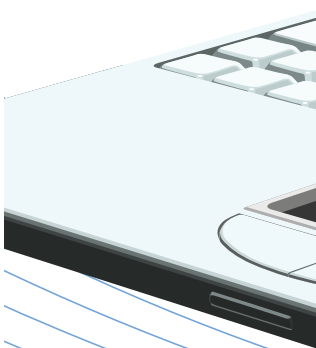
Our economic activities, social lives, and even our physical safety increasingly depend on computers and other devices linked through the Internet. Protecting those systems and the information they contain has thus become a national imperative. As President Obama said near the outset of his Administration, "America's economic prosperity in the 21st century will depend on cybersecurity."

In the past decade, an increasingly sophisticated cybersecurity industry has grown up to help companies, individuals, and government agencies contend with the growing array of threats posed by cyber attackers and cyber thieves. A recent PricewaterhouseCoopers study puts spending on cybersecurity in the United States at $30 billion a year, and growing at 10 to15 percent a year.

The legal system has been slower to respond. But legislators and law enforcement, at both the federal and state levels, have begun to pay attention, and 2012 and 2013 may well see major developments in the legal regime governing cybersecurity.

At this point, cybersecurity has become a top priority in the federal government's national security agenda, both in the executive branch and on Capitol Hill. At the same time, we have seen increased regulatory and enforcement initiatives.

In 2011 and 2012, the number of regulatory and enforcement initiatives designed to strengthen cyber defenses – prosecutions, interagency collaborations, public-private partnerships – has increased significantly. That trend is likely to accelerate, particularly in critical infrastructure sectors like energy, telecommunications, finance, defense and internet infrastructure. Regulators not normally associated with data security, such as the SEC and state insurance commissioners, are getting into the act.



We've also seen increased litigation. Many of the relevant existing statutes – such as the Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA) – were written in the pre-Internet era, indeed even before personal computers and email had become pervasive in the workplace. A similar time line applies with respect to the common-law causes of action that plaintiffs are relying on to pursue data security breach claims.

Thus, courts are still hashing out basic issues of defining who can sue and for what. This year may see a number of these issues – who has standing to sue, what kinds of damages are cognizable, and what kinds of contractual arrangements give rise to implicit guarantees of data security protection – reach state supreme courts and the U.S. Supreme Court.

New federal legislation remains a possibility. In the fall of 2011, many observers thought substantial cybersecurity legislation had a good chance of being enacted in the 2012 congressional session. Then congressional efforts were derailed by partisan divisions, business concerns about new regulations, and public anxiety about enhanced threats to on-line privacy. However, we are likely to see a renewed push for federal legislation in 2013, once the presidential election is behind us.

Regulators not normally associated with data security, such as the SEC and state insurance commissioners, are getting into the act.

Jamie Gorelick is a partner at WilmerHale. She has represented diverse interests in complex civil and criminal litigation, internal corporate investigations and counseling on issues at the intersection of law, policy and governance. She has been on numerous government commissions and panels, including the 9/11 Commission, and is a former Deputy Attorney General of the U.S. and former general counsel of the Defense Department. She is a member of the Executive Counsel Editorial Advisory Board.
jamie.gorelick@wilmerhale.com

VARIETY OF THREATS

More than two billion people use the Internet, which contains roughly 300 million websites. The number of devices other than personal computers – including cell phones, BlackBerries, and tablets – linked into the Internet is growing rapidly and creating new openings for malicious cyber activities.

Attack and Espionage. The military and intelligence agencies have turned greater attention to preventing and responding to attacks by foreign adversaries, whether hostile nations, terrorist groups, or politically motivated "hacktivists," such as Anonymous. May 2010 saw the creation of a distinct military Cyber Command, headed by a four-star general and dedicated both to protecting military computer systems and carrying out military activities in cyberspace.

Theft of Intellectual Property. Cyber theft of intellectual property, particularly by individuals and organizations in China, Russia, and former Warsaw Pact countries, has skyrocketed, with the value of stolen IP estimated in the billions of dollars.

Theft of Money. Cybercriminals are devising more sophisticated ways of manipulating computer users for illicit profit. One example: In November 2011, the FBI and the U.S Attorney's Office for the Southern District of New York announced the indictment of seven individuals connected to an Estonian company called Rove Digital, which had legitimate operations but also was accused of developing a botnet computer worm that had infected more than four million computers world-wide, and more than 100 U.S. servers. The botnet is alleged to have enabled Rove Digital to reap millions of dollars in illicit revenue by diverting users, without their knowledge, from legitimate advertisements to fake sites.

Disclosure of Personally Identifiable Information. Banks and payment service companies have been frequent targets because they possess individuals' financial information, but no sector has been immune. As many financial institutions have hardened their defenses, cyber-criminals have increasingly set their sights on other sectors, including retail, hospitality, entertainment, health care, education and social media. Breaches may result not only from cyber intrusions, but also from inadequate physical security that results in stolen or lost computers or back up media.

Insurance. The increasing frequency and severity of data security breaches are leading to increased interest in insurance products designed to help companies cope with attendant remediation and litigation costs – and to more disputes over whether existing policies cover these costs.

In the meantime, the SEC has begun to address the cybersecurity issue. On October 13, 2011, its Division of Corporation Finance issued guidance on disclosure obligations relating to cybersecurity risks and incidents. The guidance notes negative consequences public companies may encounter after a cyber incident. They include costs of remediation, costs of increased cybersecurity protection measures, lost revenues, damage to reputation and litigation costs.

In light of the damage a cyber incident can cause and existing obligations to disclose information that a "reasonable investor would consider important to an investment decision," companies may be required to provide information that allows investors to understand a company's cybersecurity risks. The SEC has begun sending out inquiry letters probing whether issuer's public statements are consistent with their filings.

SECTOR-SPECIFIC INITIATIVES

Many federal efforts targeting particular economic sectors are being initiated, and more are forthcoming. One example is the Defense Industrial Base (DIB) Pilot Program, announced in June 2011. This voluntary trial enables DIB companies or their Internet service providers (ISPs) to get access to information, including classified information, about cyber threats and responses from the government. Advocates for the program see it as a model that may be expanded to other industrial sectors.

Another initiative addresses the electric grid. In 2010, the National Institute of Standards and Technology (NIST) issued a report on cybersecurity strategy and requirements for the grid. In 2011, the Federal Energy Regulatory Commission (FERC) began, but put on hold, an effort to issue a rule on grid interoperability standards. In September 2011, the Department of Energy (DOE) issued a "Roadmap to Achieve

Energy Delivery Systems Cybersecurity." Then, in January of 2012, the White House and DOE announced an Electric Sector Cybersecurity Risk Maturity Pilot, a public-private collaboration to develop a model to help secure the electric grid against cyber threats and test that model with participating utilities.

In health care, the Office of Civil Rights at the Department of Health and Human Services, in November 2011, announced a pilot program of security and privacy audits of 150 entities covered by the privacy and security rules under the Health Care Portability and Accountability Act.

In the area of telecommunications and ISPs, in March, 2012, the Federal Communications Commission issued three voluntary codes of conduct designed to help combat botnet attacks, assaults on DNS servers and internet route hijacking.

THE LITIGATION LANDSCAPE

As data breaches have become more common and more significant, related litigation has proliferated. Many of the common-law and statutory causes of action being relied on were developed for other circumstances, so parties and courts are struggling to fit them to data breach matters. Among the questions being hashed out:

Who has standing? Does disclosure of personal information, and the attendant heightened risk of identity theft, constitute sufficient injury to give a plaintiff standing to sue in federal court, or does there need to be more concrete economic harm? Federal courts of appeals have split on the issue. The Supreme Court has so far ducked the question, but it is likely to reach the high court soon.

What suffices to create an implied contractual guarantee of security? When a customer or affected third party has no contractual agreement with the company suffering the breach, when can they nonetheless sue based on an implied contractual guarantee that the company would have adequate cybersecurity protections in place?

Many of these claims turn on the particular state's contract-law doctrines. However, a number of courts have found such a contract implied, reasoning that a customer using a credit card does not expect the merchant to allow unauthorized third-parties to access that data.

May failure to provide adequate security violate consumer protection statutes? Again, the answer will turn on the particulars of a state's consumer protection laws, but at least some courts are letting such claims proceed.

What constitutes cognizable damage? This issue is arising in a number of contexts, including state common law claims, state statutory claims, the federal Computer Fraud and Abuse Act, and the federal Privacy Act, under which the Supreme Court held (in March of this year) that mental and emotional distress from disclosure of personal medical information does not constitute "actual damages."

Theft by former employees. During the second week in April, 2012, two federal courts of appeal restricted the use of several federal statutes as tools to target those who steal data or computer code. In *United States v. Nosal*, the en banc Ninth Circuit, by a vote of 9-2, limited the reach of the CFAA by holding that gaining authorized access to information on a computer system and then using the information for a purpose prohibited by a computer-use agreement, even for a fraudulent purpose, does not constitute "exceed[ing] authorized access." In *United States v. Aleynikov*, the Second Circuit held that theft of computer source code itself could not be prosecuted under the Economic Espionage Act or the National Stolen Property Act.

FEDERAL LEGISLATIVE EFFORTS

In the fall of 2011, both President Obama and Senate Majority Leader Harry Reid (D-Nev.) identified cybersecurity as a top legislative priority, particularly in three areas: critical infrastructure protection, information-sharing and reorganization of the federal government's own cyber defenses.

House Republicans responded with their own proposals. National security experts of both parties argued that new federal laws were needed. But partisan divisions, business concerns about additional regulatory burdens, and public worries about enhanced threats to online privacy left the 112th Congress unable to adopt substantial new standards before recessing for the summer.

The depth and variety of cyber threats facing U.S. companies will only increase. In the legislative arena, as in regulatory and enforcement action and litigation, we are certain to see re-invigorated efforts in 2013, once the presidential election is behind us. ■

Jonathan Cedarbaum is a partner at Wilmer Hale He has a diverse litigation practice, focusing especially on antitrust, False Claims Act (FCA), Federal Arbitration Act, and international cases. He also counsels on administrative law and constitutional issues, particularly in transnational matters, and has particular expertise representing clients before the Committee on Foreign Investment in the United States (CFIUS). He rejoined the firm in 2011 after two years in DOJ's Office of Legal Counsel, ultimately serving as Acting Assistant Attorney General in charge of the office.
jonathan.cedarbaum@wilmerhale.com