Data Security — What Are The Issues?

By Al Saikali on August 26th, 2011

Posted in Cloud Computing, Data Security

As “the cloud” becomes an increasingly important and more widely used tool for computing and data storage, companies (and their lawyers) must address a number of challenging issues. Some of these issues include but are certainly not limited to:

- How does a company minimize the risk of data breach and maximize the security of their data at a “reasonable” cost? What level of security strikes a balance between practicality, financial reasonableness, and protection?

- What policies should a company adopt to help ensure the security of its data while maintaining the privacy rights of its employees?

- How can a company maximize the security of its customers’ private information, particularly if the information is stored in the cloud? What are the minimum standards, if any, that the law requires of a company seeking to store information in the cloud with respect to ensuring the security of their customers’ information? Are there any legal requirements or customs that a company should expect a third-party cloud vendor to meet?

- What role will the law of other countries play in regulating data stored in the cloud, particularly where a cloud vendor may store information in servers all over the world?

- What are the emerging trends in litigation? What causes of action are being brought successfully against cloud vendors and businesses that use them when a customer’s private information has been breached? Which defenses have been successful in limiting liability? What does a customer have to show to establish the existence of a cognizable injury?

It does not appear that there are easy answers to many of these questions. What does appear clear, however, is that corporations and individuals are increasingly moving their data and computing platforms into the cloud. So at the very least these issues should be considered and they create a potential minefield ripe for litigation.

It is hoped that this blog will serve as a forum for discussion of these and other issues relating to the law regulating data security, cloud computing, data privacy, and “all things E.”

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Data Security Law Journal
Shook, Hardy & Bacon, L.L.P.
2400 Miami Center
201 S. Biscayne Blvd.
Suite 3200
Miami, FL 33131-4332
P: 305.358.5171
F: 305.358.7470
Copyright © 2012, Al Saikali. All Rights Reserved. Strategy, design, marketing & support by LexBlog
Why Should You Care About Data Breaches?

By Al Saikali on September 2nd, 2011

Posted in Data Breach

Some of the most alarming statistics concerning data breaches relate to how frequently they occur, who is suffering them, and the cost such breaches impose on their victims.

According to a recent survey of 583 IT practitioners (more than half of whom were employed by organizations with more than 5,000 employees), 90% of organizations had suffered at least one data breach in the last year, 59% said they suffered two or more breaches in the last year. The cost can be staggering. According to a one study, the average organizational cost of a data breach in the United States was $7.2 million and cost companies an average of $214 per record compromised.

If nothing else, these statistics tell us why businesses of any size should care about this issue – data breaches are happening to almost everyone, they’re happening now, and they’re expensive. Technology is making the world increasingly “flat.” It is easier to disseminate large quantities of data in shorter periods of time over larger geographical areas. There is no sign that this trend will reverse itself.

So we should probably assume that as a result, more and more organizations will become susceptible to data breaches. In addition, as the security threats increase and become more complex, the costs associated with defending against such threats will also increase. Based on the above studies, it appears that larger organizations are no more immune to such attacks simply because of their size.

What steps are you taking to protect yourself? What policies and preventative measures are your company taking to minimize the risk of a data breach and, as a consequence, the exposure of its customers’ private information to the outside world?

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.
Data Breach — What’s the Harm??

By Al Saikali on September 9th, 2011

Posted in Data Breach

A data breach can result in the exposure of private customer information (credit card information, social security numbers, email addresses, etc.) to unknown third parties who may fraudulently use that information. In instances where the information is used fraudulently, the customer suffers a harm that can usually be quantified or measured in some way.

But what happens when the harm to the consumer is harder to quantify? Does a plaintiff have the necessary standing or harm to bring a lawsuit? More specifically, does the customer’s private information have its own separate, inherent value that is diminished by the data breach?

At least one federal District Court recently addressed these issues and determined that yes, the private information a consumer provides a company in exchange for the company’s services may have its own inherent value for the purpose of determining whether the plaintiff has suffered harm.

In Claridge v. RockYou, Inc., the plaintiff, Mr. Claridge, was informed by the defendant, RockYou, a developer of applications for social networking sites, that his personal information including his email address, passwords, and login credentials for social networks like MySpace and Facebook might have been compromised through a security breach. Claridge filed a class action lawsuit against RockYou based on the data breach. RockYou moved to dismiss, arguing that Claridge lacked standing and suffered no injury as required for the underlying causes of action. Claridge responded with “a novel theory” that he paid for RockYou’s services by providing his private information, and that the private information is inherently valuable. He argued that as a result of the breach, RockYou caused plaintiff to suffer diminished “value” of his private information.

The court expressed its “doubts about plaintiff’s ultimate ability to prove his damages theory” but it nevertheless rejected RockYou’s standing argument, reasoning that there was no controlling authority one way or the other regarding the legal sufficiency of Claridge’s damages theory. The court noted that “the context in which plaintiff’s theory arises—i.e., the unauthorized disclosure of personal information via the Internet—is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts.” The court did, however, dismiss several of Claridge’s counts for failure to allege the more particularized injury required for those causes of action.

The RockYou decision is important for a number of reasons, including because it appears to be one of the first to address this issue of valuing private information. It is unclear whether RockYou will start a new trend or be an outlier, but it will be interesting to look back several years from now to see what sort of impact it has had on the development of data security law.

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Data Security Law Journal
Shook, Hardy & Bacon, L.L.P.
2400 Miami Center

Data Threats Posed By “Multi-Tenant” Infrastructure In The Cloud

By Al Saikali on October 1st, 2011

Posted in Cloud Computing

When a company decides to store its data in the cloud, one of the choices it must make is whether to store the information on physical resources devoted solely to its data and computing services, or share those resources with other entities who are using the same cloud provider’s services. At the risk of oversimplifying, an analogy is deciding whether to rent a house or rent a unit in a multi-tenant building. The latter option is often less expensive and, as a result, seemingly more attractive, but it may raise more security concerns because you share the same space with other renters.

A recent study entitled, “Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,” suggests there may be certain risks associated with the multi-tenant or “multiplexing physical infrastructure environment” when it comes to cloud computing. The study explains how it may be possible for an attacker to place a malicious virtual machine (“VM”) in the multi-tenant environment cloud server and then extract confidential information via a cross-VM attack. The study concludes that, “there exist tangible dangers when deploying sensitive tasks to third-party compute clouds.”

What does this mean for a company looking to store confidential information in the cloud? At a minimum, an inquiry should be made to determine whether and to what extent the company will be sharing infrastructure with other entities using the same cloud provider. If there will be a sharing of infrastructure, the study suggests a few approaches for mitigating the risks associated with such sharing. First, the cloud provider can adjust the internal structure of their services to complicate an attacker’s ability to place the VM on the same machine as its target. Also, the provider can put into place blinding techniques that minimize the amount of information that can be leaked. The only “foolproof solution,” however, is to “insist on using physical machines populated only with their own VMs and, in exchange, bear the opportunity costs of leaving some of these machines under-utilized.”

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Data Security Law Journal

Shook, Hardy & Bacon, L.L.P.
2400 Miami Center
201 S. Biscayne Blvd.
Suite 3200
Miami, FL 33131-4332
P: 305.358.5171
F: 305.358.7470

Copyright © 2012, Al Saikali. All Rights Reserved. Strategy, design, marketing & support by LexBlog
Securing Corporate Board Information

By Al Saikali on October 16th, 2011
Posted in Data Security

The findings of a recent Thomson Reuters Accelus survey entitled Better Board Governance: Communications, Security and Technology in a Global Landscape of Change raises questions about the level of security some corporations are taking (or failing to take) to protect sensitive and confidential corporate information transmitted between the corporate entity and its board members.

The survey finds that, “corporate policies and practices for managing board documents and communications may not be keeping pace with requirements for security and compliance.” Some of the problems that the survey identified include:

- **Board Papers** – 61% of all boards disseminate important board materials in paper format instead of using secure online methods like board portal tools.

- **Board Communications** – board members communicate via methods that lack any encryption. Many use public email services such Yahoo!, Gmail, and Hotmail to conduct important board business. A significant number of board members print out their materials and carry them with them, exposing the materials to loss or theft and no ability to destroy them remotely.

- **Document Retention & Discovery** – board members are storing corporate documents on their private home computers and private mobile devices, so the documents may not be captured in response to a discovery request.

- **Secure Communications** – board members are not provided secure computing/communication devices.

- **Security** – board documents are accessible via unsecured wifi networks, exposing them to theft or hacking. A significant number of board members have reported that their laptops, mobile devices, or sensitive docs were lost, stolen, or left in public places.

- **Increased International Role** – two-thirds of board members are managing global issues for their company and 83% of companies have board members who travel internationally extensively. This raises the issues of how board members are communicating and accessing their materials overseas and what measures are in place to ensure that the international communications and transmission of materials are secure.

The survey’s findings raise several questions. For example, with board members increasingly traveling overseas and managing international issues, are data security measures only as good as the protection available in the countries where board members are traveling? What is the right balance between security and business needs? To many board members, the convenience of access to all of their business information on one device may outweigh the security risk and the expense of implementing certain security measures. What policies and procedures are in place to ensure that “sufficient” data security measures are being taken?

Perhaps the best “takeaway” from this study is that there may be a gaping hole in the protection of corporate board communications and materials. Corporate in house counsel should be aware of the risks and perhaps work with the company’s IT department to evaluate the most cost-effective options to secure corporate board information.

*DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or*
its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Data Security Law Journal

Shook, Hardy & Bacon, L.L.P.
2400 Miami Center
201 S. Biscayne Blvd.
Suite 3200
Miami, FL 33131-4332
P: 305.358.5171
F: 305.358.7470

Copyright © 2012, Al Saikali. All Rights Reserved. Strategy, design, marketing & support by LexBlog
Private Civil Lawsuits Arising From Data Breaches

By Al Saikali on October 30th, 2011

Posted in Data Breach, Data Breach, Data Security

The U.S. Circuit Court of Appeals for the First Circuit recently weighed in on the causes of action and damages that are (and are not) cognizable in a data breach case. In Anderson v. Hannaford Bros. Co., No 10-2384 (1st Cir. Oct. 20, 2011), the plaintiffs were customers of a grocery store chain. The grocery store chain used an electronic payment processing system that was breached by hackers, allowing the hackers to steal up to 4.2 million credit and debit card numbers and identifying information of the stores’ customers. Many of the plaintiffs had unauthorized charges against their credit/debit card accounts. Several were charged replacement card fees by their banks to replace their credit/debit cards. The customers sued the grocery store chain.

The plaintiffs’ lawsuit was based on several causes of action: breach of implied contract, breach of implied warranty, breach of duty of a confidential relationship, failure to advise customers of the theft of their data, strict liability, negligence, and violation of Maine’s Unfair Trade Practices Act. In its 35-page opinion, the First Circuit analyzed each of these causes of action and held that only the negligence and implied contract causes of action were viable.

The Plaintiffs sought various types of damages, including the cost of replacement cards, fees for accounts overdrawn by fraudulent charges, fees for altering pre-authorized payment arrangements, loss of accumulated reward points, inability to earn reward points during the transition to a new card, emotional distress, time and effort spent reversing unauthorized charges and protecting against further fraud, and costs incurred for purchasing identity theft/card protection insurance and credit monitoring services. The First Circuit held that only the plaintiffs’ claim for mitigation expenses (like the consumer’s purchase of credit reports or credit insurance) and card replacement costs consumers incurred were recoverable.

Civil lawsuits arising from data breaches are a new and developing area of the law, and this new opinion is important because it is among the first U.S. Circuit Court opinion to analyze the issues of the proper causes of action and recoverable damages, and to do so in depth. The decision is also important because, as journalist Jaikumar Vijayan wrote in an article for Computerworld, the case is “a rare instance of a court siding with consumers in a data breach lawsuit.” It is certainly worth a read for anyone interested in these issues, and it should be an exciting time for anyone who practices in this area because we are watching the law develop from the beginning.

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Data Security Law Journal

Shook, Hardy & Bacon, L.L.P.
2400 Miami Center
201 S. Biscayne Blvd.
Suite 3200
Miami, FL 33131-4332
P: 305.358.5171
F: 305.358.7470

Copyright © 2012, Al Saikali. All Rights Reserved. Strategy, design, marketing & support by LexBlog

Obligation to Disclose Security Risks

By Al Saikali on December 20th, 2011

Posted in Data Security

What obligation does a publicly traded company have to disclose security breaches? On October 13, 2011, the Securities and Exchange Commission took an important step towards answering this question when it issued a guidance that attempts to clarify a company’s obligations to disclose cybersecurity risks in registration statements and periodic reports required by the Securities Exchange Commission.

The “CF Disclosure Guidance: Topic No. 2” provides the SEC’s Division of Corporation Finance’s views regarding disclosure obligations relating to cybersecurity risks. Publicly traded companies are required to disclose timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision. The guidance clarifies that this same obligation may apply to cybersecurity risks and incidents if the issues those risks/incidents raise “are among the most significant factors that make an investment in the company speculative or risky.”

In determining whether a risk factor disclosure is required, a company should consider the severity and frequency of prior cyber incidents, including the potential costs and other consequences resulting from misappropriation of sensitive information, corruption of data, or operational disruption. The company should also 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.”

The guidance also provides instruction on what an appropriate disclosure should contain once a company has determined that a disclosure is necessary:

- Discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

In my next post, we will look at the limitations of the Guidance.

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.
Limitations of the SEC Guidance on Disclosure of Cyber Security Risks

By Al Saikali on December 22nd, 2011

My previous post discussed the SEC’s Division of Corporation Finance’s recent Corporate Finance Disclosure Guidance which provides the Division of Corporation Finance’s views regarding disclosure obligations relating to cybersecurity risks and cyber incidents. There are limitations to this Guidance, and this post attempts to address some of those limitations.

One limitation is the legally binding effect of the Guidance. The Guidance states that it “is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.”

Another limitation is to whom the Guidance applies. The Guidance applies to registrants with the SEC (i.e., publicly traded companies). These are entities that must file registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934.

The Guidance also limits what information must be disclosed. For example, a company is not required to disclose information that would compromise a registrant’s cybersecurity. “Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.”

The Guidance also limits the amount of detail that must be provided as part of the disclosure in an effort to prevent providing a roadmap that would make future cyber attacks easier: “We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts – for example, by providing a 'roadmap' for those who seek to infiltrate a registrant’s network security – and we emphasize that disclosures of that nature are not required under the federal securities laws.”

In short, a company that has suffered a cyber attack or risks of a cyber attack, should consider the application of the CF Disclosure Guidance: Topic No. 2, but the company should not automatically assume that the Guidance applies to them, and care should be taken to ensure that, to the extent a disclosure is required, it is narrowly tailored to provide the type of information required by the Guidance.

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Data Security Law Journal

Shook, Hardy & Bacon, L.L.P.
2400 Miami Center
201 S. Biscayne Blvd.
Suite 3200
Miami, FL. 33131-4332
P: 305.358.5171
F: 305.358.7470

Copyright © 2012, Al Saikali. All Rights Reserved. Strategy, design, marketing & support by LexBlog

http://www.cloudcomputinglawjournal.com/2011/12/22/data-security-%e2%80%93-limitat... 3/12/2012
Foreign Economic Cyber-Espionage (Part 1)

By Al Saikali on March 1st, 2012

Posted in Data Security

This blog entry begins a multi-part series on the rise of foreign economic cyber-espionage. In October 2011, the U.S. Office of the National Counterintelligence Executive issued a report to Congress entitled “Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.” The report was significant because it was one of the first formal documents in which the U.S. government took a clear position that elements in China and Russia are actively and intentionally stealing U.S. economic secrets through the use of cyber attacks. The Chairman of the House Intelligence Committee told the New York Times that “[t]he biggest threat, when it comes to cyber-espionage today, is the sheer volume with which China seeks to steal our intellectual property for its own prosperity.”

The report details the “cyber collection” of information by foreign actors, which can take many forms, like simple visits to a U.S. company’s website for the collection of openly available information, a corporate insider’s downloading of proprietary information onto a thumb drive at the behest of a foreign rival, or intrusions launched by foreign intelligence services or other actors against the computer networks of a private company, federal agency, or an individual.

The report provides examples of how a massive number of computer network intrusions have been used to attack U.S. corporations, primarily in the health care, pharmaceutical, and defense industries. The report concedes, however, that attribution to a specific country can be difficult because it is often based on circumstantial evidence, such as the fact that the IP addresses for these computer network intrusions originate in that country.

Some examples of cyber-espionage documented in the report include:

- In a February 2011 study, McAfee attributed an intrusion set they labeled “Night Dragon” to an IP address located in China and indicated the intruders had exfiltrated data from the computer systems of global oil, energy, and petrochemical companies. Starting in November 2009, employees of targeted companies were subjected to social engineering, spear-phishing e-mails, and network exploitation. The goal of the intrusions was to obtain information on sensitive competitive operations and on financing of oil and gas field bids and operations.

- In January 2010, VeriSign iDefense identified the Chinese Government as the sponsor of intrusions into Google’s networks. Google subsequently made accusations that its source code had been taken—a charge that Beijing continues to deny.

- Mandiant reported in 2010 that information was pilfered from the corporate networks of a US Fortune 500 manufacturing company during business negotiations in which that company was looking to acquire a Chinese firm. Mandiant’s report indicated that the US manufacturing company lost sensitive data on a weekly basis and that this may have helped the Chinese firm attain a better negotiating and pricing position.

- Participants at an Office of National Counterintelligence Executive conference in November 2010 from a range of US private sector industries reported that client lists, merger and acquisition data, company information on pricing, and financial data were being extracted from company networks—especially those doing business with China.

In addition to Chinese economic espionage, the report also cites the June 2010 arrest of ten Russian foreign intelligence service employees who were tasked with collecting economic and technology information. In certain cases, according to the report, allies and other countries enjoy broad access to U.S. Government agencies and the private sector and conduct economic espionage to acquire sensitive U.S. information and technologies.
Future entries in this series will focus on the cost of these cyber attacks on the U.S. economy and what is being done to limit it.

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Data Security Law Journal
Shook, Hardy & Bacon, L.L.P.
2400 Miami Center
201 S. Biscayne Blvd.
Suite 3200
Miami, FL 33131-4332
P: 305.358.5171
F: 305.358.7470

Copyright © 2012, Al Saikali. All Rights Reserved. Strategy, design, marketing & support by LexBlog
Foreign Economic Cyber-Espionage (Part 2)

By Al Saikali on March 1st, 2012

Posted in Data Security

This series of blog entries on foreign economic cyber-espionage arose from a recent government report detailing the source, extent, and threat of cyber-espionage to the U.S. economy. This entry focuses on the cost of this espionage to the U.S. and global economy.

The National Counterintelligence Executive report finds that the threat of cyber-espionage applies to all U.S. economic activity and technology, but the greatest threats are to:

- Information and communications technology, which forms the backbone of nearly every other technology.
- Business information that pertains to supplies of scarce natural resources or that provides foreign actors an edge in negotiations with U.S. businesses or the U.S. Government.
- Military technologies, particularly marine systems, unmanned aerial vehicles, and other aerospace/aeronautic technologies.
- Civilian and dual-use technologies in sectors likely to experience fast growth, such as clean energy and healthcare/pharmaceuticals.

With respect to the health care and pharmaceutical industry, the report specifically notes that, “The massive R&D costs for new products in these sectors—up to $1 billion for a single drug—the possibility of earning monopoly profits from a popular new pharmaceutical, and the growing need for medical care by aging populations in China, Russia, and elsewhere are likely to drive interest in collecting valuable U.S. healthcare, pharmaceutical, and related information.”

Cyber-espionage has cost tens or hundreds of millions of dollars in potential profits to U.S. entities, but the report also identifies several factors that affect the cost of cyber-espionage:

- Many victims of economic espionage are unaware of the crime until years after loss of the information.
- Even when a company knows its sensitive information has been stolen by an insider or that its computer networks have been penetrated, it may choose not to report the event to the FBI or other law enforcement agencies. No legal requirement to report a loss of sensitive information or a remote computer intrusion exists, and announcing a security breach of this kind could tarnish a company’s reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders.
- A company also may not want to publicly accuse a corporate rival or foreign government of stealing its secrets out of fear of offending potential customers or business partners.
- Finally, it is inherently difficult to assign an economic value to some types of information that are subject to theft. It would, for example, be nearly impossible to estimate the monetary value of talking points for a meeting between officials from a U.S company and foreign counterparts.

Nicole Perlroth, a reporter for the New York Times Bits column, writes regularly on data privacy and data security issues. She recently reported on the issue of economic cost of economic cyber-espionage in greater depth. In an article titled “How Much Have Foreign Hackers Stolen?” she points out that nobody really knows how much has been stolen and, predictably,
companies are reluctant to discuss any security breaches they have suffered. Her research, however, identified Congressional testimony by the Assistant Director of the U.S. Secret Service estimating that in 2010 “cyberthieves abroad stole 867 terabytes of data from the United states, or nearly four times the amount of data collected in the archives of the Library of Congress.” That amount is now stolen on a daily basis, according to the former Director of National Intelligence. Any computer system of consequence has been compromised by an advanced persistent threat.

The problem will only get worse as foreign technology improves, more data is moved into “the cloud”, and workers make it easier to steal trade secrets by carrying them around with them on their personal devices. Ms. Perlroth wrote a separate article called “Traveling Light in a Time of Digital Thievery” that describes the extent to which companies are going to protect their data when their employees travel abroad. Such measures include bringing loaner devices that are wiped clean before they leave the U.S. and immediately upon return to the U.S., disabling Bluetooth and Wi-Fi when overseas, and copying and pasting passwords from a separate USB thumb drive. The article is well worth a read for anyone traveling overseas with a mobile device that is used to access corporate data in the United States.

DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Data Security Law Journal
Shook, Hardy & Bacon, L.L.P.
2400 Miami Center
201 S. Biscayne Blvd.
Suite 3200
Miami, FL 33131-4332
P: 305.358.5171
F: 305.358.7470

Copyright © 2012, Al Saikali. All Rights Reserved. Strategy, design, marketing & support by LexBlog

http://www.cloudcomputinglawjournal.com/2012/03/01/data-security-foreign-economic-cy... 3/12/2012
Foreign Economic Cyber-Espionage (Part 3)

By Al Saikali on March 1st, 2012

Posted in Data Breach, Data Security

This final blog entry in the series about economic cyber-espionage focuses on what, if anything, the government can do and is doing to limit cyber attacks that result in the theft of billions dollars worth of intellectual property and confidential proprietary information.

The issue of cyber-espionage is receiving attention from the highest levels of government. For example, the report that was the basis for this series was prepared by the Office of the National Counterintelligence Executive, which is part of the Office of the Director of National Intelligence. It is staffed by senior counterintelligence and other specialists from across the national intelligence and security communities. The Intelligence Authorization Act for Fiscal Year 1995 requires that the President biennially submit to Congress updated information on the threat to U.S. industry from foreign economic collection and industrial espionage. This report was submitted to Congress pursuant to that obligation.

The issue is gaining significant attention in the U.S. media, for legitimate reasons. Loren Thompson, a contributor for Forbes magazine recently authored an article entitled “U.S. headed for Cyberwar Showdown with China in 2012.” In it, Mr. Thompson points out that even though cyber-espionage is “being executed by a relatively small number of agents linked to the general staff of China’s People’s Liberation Army, the damage they are inflicting on U.S. security and economic competitiveness is judged to be extensive.” But as Thompson points out, the question is what, if anything, can be done about it.

Part of the problem appears to be identifying precisely who is engaging in these cyber attacks. According to a report by Siobhan Gorman in the Wall Street Journal the Obama Administration has had some success in identifying some of the key operatives in the Chinese cyber campaign (though the Chinese claim that such allegations are “totally ungrounded” and that Chinese law “clearly prohibits hacking”). I highly recommend the article to anyone interested in a deeper investigation into allegations of Chinese cyber-espionage.

Yet, Mr. Thompson with Forbes posits, the administration has taken little offensive action against China because “it doubts confrontational tactics will produce positive results.” But given the billions dollars in economic information being lost to the Chinese intrusions and the possibility of far worse attacks, it is far more likely that the administration will be forced to be more openly aggressive.

In addition to the issue increasingly gaining the attention of the executive branch, Congress is considering competing legislation that would seek to limit the risk or cyber attacks. The Cybersecurity Act of 2012 (S.2105), introduced by Senators Lieberman and Rockefeller, would give the Department of Homeland Security regulatory authority over companies with computer systems crucial to the nation’s economic and physical security. Republicans have proposed alternative legislation called the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act (“SECURE IT”). Crudely defined, the Republican alternative relies on companies voluntarily sharing threat data through certain cybersecurity centers. In exchange, companies would receive incentives, such as protection from civil lawsuits and exemption from public disclosure. It is unclear whether Congress will ultimately pass either piece of legislation.

UPDATE: 60-Minutes recently aired a very interesting story on the Stuxnet virus, which is a virus believed to have been used offensively to attack Iranian nuclear plants. The piece is particularly relevant to this series of blog entries because it discusses the increased trend in international espionage through cyber attacks. I highly recommend the story to those of you interested in this issue.

http://www.cloudcomputinglawjournal.com/2012/03/01/data-security-foreign-economic-cy... 3/12/2012
DISCLAIMER: The opinions expressed here represent those of Al Saikali and not those of Shook, Hardy & Bacon, LLP or its clients. Similarly, the opinions expressed by those providing comments are theirs alone, and do not reflect the opinions of Al Saikali, Shook, Hardy & Bacon, or its clients. All of the data and information provided on this site is for informational purposes only. It is not legal advice nor should it be relied on as legal advice.

Tags: cyber-espionage, cybersecurity

Data Security Law Journal

Shook, Hardy & Bacon, L.L.P.
2400 Miami Center
201 S. Biscayne Blvd.
Suite 3200
Miami, FL 33131-4332
P: 305.358.5171
F: 305.358.7470

Copyright © 2012, Al Saikali. All Rights Reserved. Strategy, design, marketing & support by LexBlog