ASA

Annie Searle & Associates LLC

Research Note

Cybersecurity in the U.S. Private Sector

Mark Tchao

March 2016

Keywords: Private Sector, Cybersecurity, Privacy, Data Breach, Intellectual Property, Critical Infrastructure, National Security

Abstract: Despite its perpetual resurfacing in the media, the prevalence of cyber-attacks on American companies is no grounds to excuse them– data breaches affect the privacy and financial security of millions of people, disrupts economic prosperity, and are arguably the largest threat to national security. While massive retailers or utility providers never imagined to be liable for the well-being of an entire country, reality proves otherwise. Incentivizing companies to invest in top cybersecurity measures in the profit-driven market continues to be a challenge and government compliance can be illusory, but without decisive changes in the landscape of matters, things may only get worse.

The State of Affairs

"There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese," said FBI Director James Comey in an interview with CBS "60 Minutes."[1] But the threat of hackers extends beyond just the Chinese– criminal organizations and nation-state actors across the globe are increasingly targeting the Western private sector, hoping to capitalize from stolen personal information intellectual property, and even attempt to control infrastructural systems.[2] While it may be consoling to believe that the public sector is solely responsible for the security of its people– online or otherwise– the truth is that it is simply not the case. It is largely within the chaotic realm of the private sector that our privacy, our finances, and our safety lies.

Data breaches involving personal customer information tend to receive the most publicity, with high-profile incidents involving large corporations making headline news. Major companies such as Target, Home Depot, JPMorgan Chase, and Anthem have all experienced massive data

breaches leading to the compromising of hundreds of millions of personal records. In the Target hack alone, 70 million records of its customers were stolen, including 40 million credit and debit card numbers.[3] In the JPMorgan Chase hack, 76 million households and 7 million small businesses were impacted, making it one of the largest data breaches in the finance industry.[4]

The list of companies goes on: Home Depot had 109 million records involving credit card numbers compromised, Ebay had 145 million records involving login credentials and addresses stolen, Anthem had personally identifiable information (PII) involving social security numbers for 80 million people stolen– and these are just the significant breaches.[5] Virtually every major business in the U.S. has experienced a data breach, whether they are aware of it or not, leaving millions of people vulnerable to fraud and theft.

Data breaches involving intellectual property and trade secrets tend to receive less public attention, though devastating nonetheless. One high-profile example, however, is the Sony hack where business information as well as plans and copies of unreleased films were compromised. But Sony, along with virtually every other major technology firm, and many companies within the pharmaceutical and manufacturing industries have experienced hacks involving intellectual property.[6] Often times these attacks are perpetrated by Chinese hackers who sell the stolen information to companies, who then, due to strong production capabilities and lack of regulation in China, introduce these products into the market before the original creators do.

This can be devastating for a company, as seen with the bankruptcy of Nortel, which was once a leading multinational telecommunications and network equipment manufacturer based in Canada, having once controlled 40% of the telecommunications infrastructure in the United States.[7] For almost ten years, Chinese hackers exfiltrated critical intelligence, including research and development (R&D) reports, business plans, and technical documents. After continually losing profits and being forced to lay off employees, Nortel filed for bankruptcy in 2009; all the while Chinese competitors concurrently burgeoned.[8] There is no clear indication as to whether the Chinese competitors themselves compromised the data or whether Nortel's bankruptcy was caused by this corporate espionage, the correlation is hard to ignore. Cyber theft of intellectual property can be a national security concern as well, such as when Chinese hackers stole critical secrets from Lockheed Martin regarding information on their F-35 Lightning II stealth fighter jet, allowing the Chinese government to replicate a stealth fighter of their own.[9]

Yet a more crucial though often overlooked victim of cyber attacks within the private sector is infrastructural and public safety control systems. With 85% of the United State's critical infrastructure being privately-owned, it is important for the safety of the country that the companies that run the critical infrastructure prevent malicious attackers from gaining access to these systems.[10] And the risk of cyber attacks to infrastructure is completely feasible– demonstrated in examples such as the Saudi Aramco hacks, which severely disrupted oil production in Saudi Arabia, and Stuxnet, which targeted Iranian uranium enrichment facilities.[11] The Stuxnet hack serves to be an especially ominous case as it had the full capacity and sophistication to cause a nuclear meltdown, and yet it opted for a more discreet intent to slowly

degrade the centrifuges within the enrichment facilities.[12] If advanced hostile nation-states desired to cause massive damages and loss of life by target nuclear facilities within the United States, it is completely within the realm of possibility to do so– even by simply taking Stuxnet's code and weaponizing it.

In recent news, ISIS has been attempting to attack the United State's power grid, and though currently unsuccessful in causing damage, antiquated security controls within the energy infrastructure are not difficult to find.[13] And this risk to public safety extends beyond infrastructural systems. A group of researchers demonstrated that they could remotely killed the brakes on a Jeep Cherokee while it was driving down a highway, revealing the possibility of malicious actors threatening public safety on the streets.[14] Though it is unclear how tangible of a threat vehicle hacking will be in the future, to ignore the risk is a luxury we cannot afford.

The Cost of Insecurity

The cumulation of cyber criminal activity costs both businesses and consumers substantial amounts of money. A study conducted by the Ponemon Institute of Cyber Crime indicated that cyber breaches cost each average American firm about $15.4 million every year.[15] This average is double the average for firms outside of the United States. The study also estimated that about $160 billion worth of intellectual property is stolen from Western companies every year.[16] Overall, cyber criminal activity costs both businesses and consumers $400 billion a year, and one fourth of this total is believed to be from the United States alone. A report by McAfee estimated that over 500,000 American jobs have been lost due to cyber attacks since the report was published in 2013.[17] So in addition to the damages to privacy of personal information, business continuity, and public safety, an insecure private sector becomes a significant financial burden to both businesses and consumers alike.

Yet despite of these facts, most companies are not impelled to invest in premium security systems and practices due to a lack of a financial incentive.[18] Investing in cybersecurity controls can be a multimillion dollar expense, and researchers at the Pardee Center for International Futures believe that by 2019, the cost for security systems will outweigh its actual benefits.[19] The business leaders in the private sector are often unwilling to spend large amounts of money on security for what they believe is a chance that their companies would get hacked. And for many companies, the cost of a data breach do not even outweigh the continuous significant investment in security systems in the first place. "You can spend an infinite amount on security," says Robert Carr, CEO of Heartland Payment Systems Inc., "Where do you draw the line?"

It is within this obscure assumption of adequacy that leads business leaders to place their full confidence in complying to government security standards and regulations. However, compliance to government initiated standards are widely considered to be mere an illusion of security, and may often conflict with ideal security goals.[20] Furthermore, the government has an equally poor track record of an inability to keep secrets, with examples like the Chelsea Manning leak, the Edward Snowden leak, the OPM breach, the Pentagon breach, and other incidents. In order to foster innovation and encourage businesses to improve security beyond the bare

minimum, there needs to be fundamental and collaborative changes within both the private and public sectors.

Changing the Landscape

Regarding changes within the private sector, insurance companies should underwrite rates based on cyber risk assessments. Because all publicly traded companies are required to invest in cybersecurity insurance, the insurance companies have the ability to incentivize businesses to reduce their security risk in order to save more money on insurance. Continual risk-based assessments will accumulate a good understanding of safe security practices, in which they could share and recommend with other companies who are assessed as high risk.

Also, businesses should focus on providing white hat incentives for uncovering security vulnerabilities within their systems. United Airlines rewarded a hacker one million air miles for responsibly notifying United Airlines of a critical zero-day Remote Code Execution (RCE) exploit within their systems, as well as other risks.[21] Rewarding hackers for uncovering security flaws is much cheaper than implementing and maintaining multimillion dollar security systems and tends to succinct. Instead of relying on blanket security controls, organizations are able to discover precise vulnerabilities within their systems. Businesses can also potentially deter black hat hackers from illegally profiting off of the company's vulnerabilities and instead turn in these discoveries for a guaranteed reward, all without breaking the law.

Additionally, companies should be endorsed for innovating practices in cybersecurity. Target experienced a 46 percent drop in profits after the 2013 hack, therefore it can be presumed that consumers are wary of the risks of data breaches and would prefer to shop where they feel their information will be safe. If market research firms like J.D. Power and Associates were to publicly reward companies for striving for the best security practices, it would reassure customers and strengthen brand value for businesses.

Regarding changes within the public sector, the government must end the war on encryption, and encryption should instead be encouraged as a common practice within business and consumers. When the National Security Agency (NSA) forced major technology firms to install crypto backdoors into their systems and products, it lead to massive vulnerabilities like FREAK (Factoring attack on RSA-EXPORT Keys).[22] A group of security researchers demonstrated that with "$104 and 8 hours of Amazon's cloud computing power" they could exploit the FREAK vulnerability to hack into the NSA's website using a Man-in-the-Middle (MITM) attack.[23] The government's fear of encryption technology and its struggle to control its implementation is not only futile– it threatens the security of everyone.

Furthermore, the government should establish an agency that moderates communication among the private sector for sharing security information. This agency should accumulate data about cyber activity and work with companies to develop better security standards and regulations, and give recommendations for top-tier security practices. With their expertise, this agency can work closely with local law enforcement to track malicious actors, and can lead investigations involving cybercrime.

Lastly, businesses should be fined more strictly for not complying to cybersecurity standards so that business leaders no longer consider data breaches to be a small financial risk. Companies should be strictly fined for data breaches, and this money should be distributed to victims as indemnities. These businesses are responsible for securing the data of its customers; therefore businesses must make amends to its consumers rather than disregard their failures.

Overall, it should not be acceptable that tens of millions of Americans have their online information compromised every year, or that businesses lose millions of dollars to cyber espionage, or that we tolerate the threat of cyber attacks causing real-world damages. Though the commonality of data breaches make them appear like a normal cost of doing business, they are a serious concern to the well-being and security of the United States. In order to better protect everyone in both the cyber and physical world, the public and private sectors must take redesigning measures to not just meet or enforce bare security requirements, but to strive for the best security practices attainable.

---

[1] Pelley, Scott. "FBI Director on Threat of ISIS, Cybercrime." *CBS News*. 05 Oct. 2014. Accessed Dec. 2015 <www.cbsnews.com>.

[2] Jortiz. "Government Needs the Private Sector to Improve Cybersecurity." *TaaSera*. Accessed Dec. 2015. <www.taasera.com>.

[3] Krebs, Brian. "The Target Breach, By the Numbers." *Krebs on Security*. 14 May 2014. Accessed Dec. 2015. <krebsonsecurity.com>.

[4] Tobias, Sharone. "2014: The Year in Cyberattacks." *Newsweek*. 31 Dec. 2014. Accessed Dec. 2015. <www.newsweek.com>.

[5] Collins, Keith. "A Quick Guide to the Worst Corporate Hack Attacks." *Bloomberg*. 18 Mar. 2015. Accessed Dec. 2015. <www.bloomberg.com>.

[6] Perez, Evan. "Security Firm: Chinese Hackers Tried to Steal Tech and Drug Companies' Secrets." *CNN Money*. 9 Oct. 2015. Accessed Dec. 2015. <money.cnn.com>.

[7] Leyden, John. "Whistleblower: Decade-long Nortel Hack 'traced to China'" *The Register*. 15 Feb. 2012. Accessed Dec. 2015. <www.theregister.co.uk>.

[8] Kehoe, John. "How Chinese Hacking Felled Telecommunication Giant Nortel." *Financial Review*. 26 May 2014. Accessed Dec. 2015. <www.afr.com>.

[9] Gertz, Bill. "Top Gun Takeover: Stolen F-35 Secrets Showing up in China's Stealth Fighter." *The Washington Times*. 13 Mar. 2014. Accessed Dec. 2015. <www.washingtontimes.com>.

[10] "Critical Infrastructure and Key Resources." *Information Sharing Environment*. 4 Feb. 2015. Accessed Dec. 2015. <www.ise.gov>.

[11] Pagliery, Jose. "The Inside Story of the Biggest Hack in History." *CNN Money*. 5 Aug. 2015. Accessed Dec. 2015. <money.cnn.com>.

[12] Kelley, Michael B. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." *Business Insider*. 20 Nov. 2013. Accessed Dec. 2015. <www.businessinsider.com>.

[13] Bender, Jeremy. "'They'd Love to Do Damage': The FBI Says ISIS Wants to Go after One of America's Biggest Vulnerabilities." *Business Insider*. 19 Oct. 2015. Accessed Dec. 2015. <www.businessinsider.com>.

[14] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway-With Me in It." *Wired*. 21 July 2015. Accessed Dec. 2015. <www.wired.com>.

[15] Griffiths, James. "Cybercrime Costs the Average U.S. Firm $15 Million a Year." *CNN Money*. 8 Oct. 2015. Accessed Dec. 2015. <money.cnn.com>.

[16] Lawrence, Dune. "The Global Cost of Cybercrime: More Than $400 Billion Per Year." *Reuters*. 09 June 2014. Accessed Dec. 2015. <www.reuters.com>.

[17] Kirchheimer, Sid. "Cybercrime Costs 508,000 U.S. Jobs." *AARP*. 25 July 2013. Accessed Dec. 2015. <blog.aarp.org>.

[18] Pasquali, Valentina. "Cover: The Untold Cost of Cybersecurity." *Global Finance*. 2 May 2013. Accessed Dec. 2015. <www.gfmag.com>.

[19] Chabrow, Eric. "Assessing the Cost of Cybersecurity." *BankInfoSecurity*. 10 Sept. 2015. Accessed Dec. 2015. <www.bankinfosecurity.com>.

[20] Miller, Wes. "How Compliance and Security Requirements May Conflict." *TechNet*. June 2008. Accessed Dec. 2015. <technet.microsoft.com>.

[21] Dastin, Jeffery. "United Airlines Awards Hackers Millions of Miles for Revealing Risks." *Reuters*. 16 July 2015. Accessed Dec. 2015. <www.reuters.com>.

[22] Abel, Jennifer. "NSA "backdoor" Mandates Lead to a Computer-security FREAK Show." *ConsumerAffairs*. 6 Mar. 2015. Accessed Dec. 2015. <www.consumeraffairs.com>.

[23] Paganini, Pierluigi. "Just $104 to Exploit the FREAK Flaw and Hit the NSA Website." *Security Affairs*. 07 Mar. 2015. Accessed Dec. 2015. <securityaffairs.co>.