NationalJournalMembership

Data Breach Primer

March 10, 2016

Producer: Justin C. Brown
Edited by: Katharine Conlon
Director: Afzal Bari

Roadmap for the Presentation

Data Breach Basics

Government Action on Cybersecurity

Examples of Major Data Breaches

Data Breaches Can Come in Many Different Forms

Types of Data Breaches

Lost/Stolen Media: Physical security is an integral part of cybersecurity. Keeping computers, hard drives, and other important technological materials safe from burglary or loss is just as important as keeping them safe from attacks through the internet.

Inside Job: Staff and other personnel with access to valuable digitized information may present a liability, as some data breaches result from staff abusing their access for personal gain.

Poor Security: Some hackers may notify organizations of poor software architecture and may attack only after the organization fails to improve their security measures. In these instances, its as though they “left the backdoor open” and haven’t taken the time to close it and install proper locks.

Hacking: While hacking still typically takes advantage of poor security architecture, more sophisticated hacking typically involves the development of a sophisticated tool, such as a virus or malware, that manages to get past even robust security measures.

Source: National Journal Research, 2016; Images by Emily Van den Heever, Luis Prado, Sebastian Langer and Effach, made available through The Noun Project.

A Poor Reaction Can Make a Bad Data Breach Even Worse

Responding to a Data Breach

It is crucial for organizations to react swiftly once a data breach has occurred to prevent further data loss

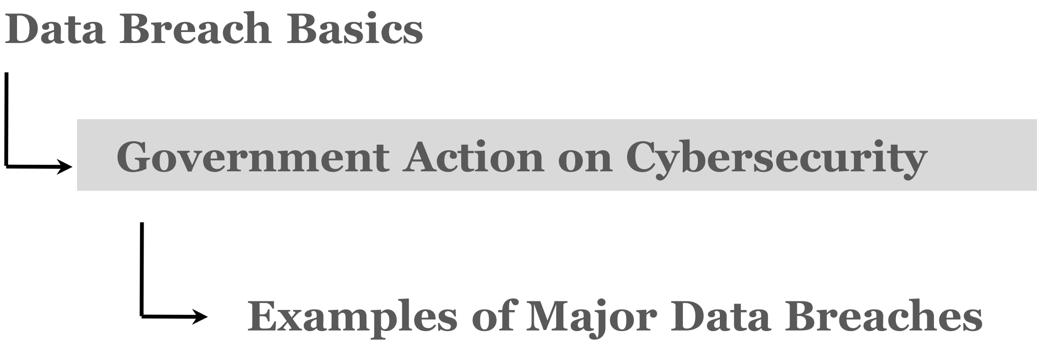
Security architecture must be enhanced to be resilient against future attacks

Organizations must thoroughly examine the nature of the breach to fully understand the scale of the attack as the amount of data lost is often initially underestimated

Typically the data that is accessed, altered or stolen is personal data of customers or employees, so it is imperative that the owners of personal data are notified so they can take necessary precautions to prevent identity theft

Source: National Journal Research, 2016; Images by Jean-Philippe Cabaraoc, Ilsur Aptokov, Gregor Cresnar; made available through The Noun Project.

Roadmap for the Presentation



Data Breach Basics

Government Action on Cybersecurity

Examples of Major Data Breaches

Recent Legislation Brings Several Government Agencies Together to Address Cyber Threats

Government Agency Roles in the Cybersecurity Information Sharing Act

- The Cybersecurity Information Sharing Act was passed in December 2015.
- **The Department of Homeland Security is designated as the central repository for cyber threat data.**
- Private companies as well as local and state governments are allowed to share this cyber threat information
- When sharing this information with the federal government, companies are offered certain liability protections from privacy lawsuits.

- **The Department of Defense, National Security Agency and the Justice Department are all allowed access to this cyber threat data.**
- Identifying details unrelated to network threats are required to be removed before sharing occurs.
- Privacy proponents fear that this will only lead to increased domestic government surveillance.
- Others in the tech world fear that amassing this information in a central location could lead to increased cyber attacks aimed at attaining this access to the database.

Source: Aliya Sternstein, "Cyber Bill Boosts DHS Cyberthreat Sharing But Critics Fear Backdoor to NSA Surveillance," Nextgov, December 18, 2015.

Encryption Remains Controversial As Evidenced by the Ongoing Battle Between Apple and the FBI

Timeline of the Apple v. FBI Encryption Dispute

Dec. 2015

San Bernardino Attack

Tashfeen Malik and Sayed Rizwan Farook kill 14 and wound 22 at the Inland Regional Center in San Bernardino, CA before dying in a shootout with police. The following day, the FBI opens a counter-terrorism investigation after ISIL named the shooters as supporters.

Feb. 2016

FBI Obtains Phone and Alerts Senate of Difficulties

James Comey tells the Senate that FBI investigators retrieved Farook's phone but due to encryption measures, they are unable to unlock the phone without possibly erasing vital user data.

Feb. 2016

US District Court Orders Apple to Develop "Backdoor" to Bypass Encryption

U.S. District Court in Los Angeles rules that Apple must provide "reasonable technical assistance" by developing a workaround that will bypass current encryption features and allow investigators use a brute force hacking method to access the data on the phone.

Feb. 2016

Apple Challenges Court Ruling, Gains Support of Larger Tech Community

Tim Cook, CEO of apple, publishes a statement which denies the court's request for Apple's compliance. Cook cites that developing this technology would put the privacy of all iPhone users at risk. Many prominent tech CEOs provide insight and support to his stance. Apple files a legal response to the FBI, asserting that the government is attempting to significantly expand powers afforded by the All Writs Act.

Mar. 2016

House Judiciary Committee Condemns FBI, Justice Department's Actions

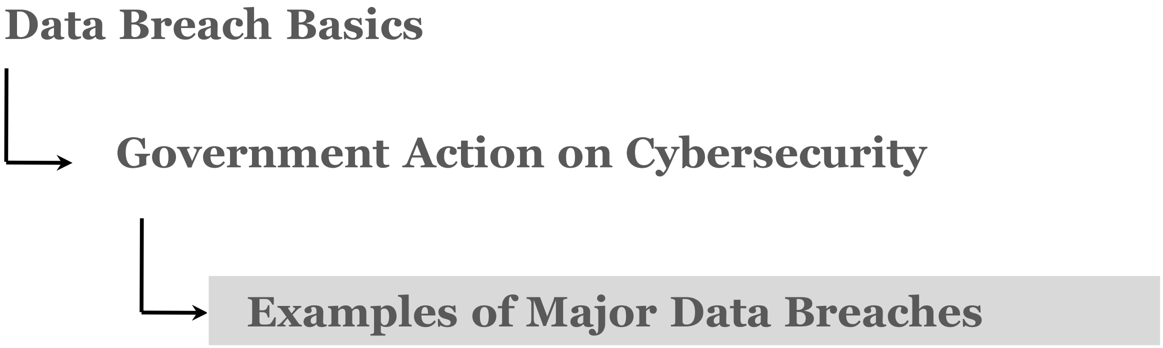
The House Judiciary Committee meets to consider the FBI's ongoing dispute with Apple and condemns their actions, disapproving of their attempts to overreach their authority. Rep. Zoe Lofgren called the demands a "fool's errand" that undermined cybersecurity.

Legislative Impact

- Rep. Michael McCaul (R-TX) and Sen. Mark Warner (D-VA) have introduced legislation which would **establish the National Commission on Security and Technology Challenges**. The goal of the commission would be to review make recommendations on policy pertaining to subjects including encryption and cybersecurity.
- Sen. Richard Burr (R-N.C.) and Sen. Dianne Feinstein (D-CA), leaders of the Senate Intelligence Committee are **currently drafting legislation aimed at giving law enforcement access to encrypted data.**

Source: Cory Bennett, "Senate Intel Encryption Bill Could Come Next Week," The Hill, March 9, 2016; David Bisson, "A Timeline of Apple-FBI iPhone Controversy," Tripwire, March 1, 2016.

Roadmap for the Presentation



Data Breach Basics

Government Action on Cybersecurity

Examples of Major Data Breaches

Local, State and Federal Governments Are All Vulnerable to Data Breaches

Recent Data Breaches at Government Agencies and Databases

Year	Agency/Database	Number of Records	Method of Leak	Description
2009	Virginia Department of Health	8,200,000	Hacked	Hackers accessed patient and prescription records, encrypted the information onto a personal server, then deleted them from the website, holding the records for a ransom of $10 million. The department relied on backup records to avoid further problems, but the hack opened the door to patient identity theft.
2012	Medicaid/Utah Department of Tech. Services	780,000	Hacked	The Utah Department of Technology Services switched its claim records data to a new server that experienced a configuration error. Hackers from Eastern Europe exploited the error to retrieve medical record information and social security numbers of hundreds of thousands of Medicaid patients.
2012	California Department of Child Support Services	800,000	Lost/Stolen Media	During a disaster simulation, a data cartridge containing addresses, driver's license numbers, and other personal data was lost in transit.
2015	Office of Personnel Management	21,500,000	Hacked	Hackers, believed to be from China, gained access to documents containing government employees' credit ratings, arrest records, bank records, family information as well as basic personal information.

Sources: Emil Protalinski, "Medicaid hack update: 500,000 records and 280,000 SSNs stolen" ZDNet, April 9, 2012. Shaya Taefe Mohajer, "Security Breach: Lost Data Cartridges May Have Exposed Personal Records From California's Child Support System," Huffington Post, March 30, 2012; Brian Krebs, "Hackers Break Into Virginia Health Professions Database, Demand Ransom," The Washington Post, May 4, 2009.; Angus Loten, "OPM Data Breach Tops List of Federal Fumbles" December 1, 2015; David Larter and Andrew Tilghman, "Military clearance OPM data breach 'absolute calamity'," Navy Times, June 18, 2015; Kim Zetter and Andy Greenberg, "Why the OPM Breach is Such a Security and Privacy Debacle," Wired, June 11, 2015. Table is Excerpt from: David McCandless, "World's Biggest Data Breaches," Information Is Beautiful.net, February 16, 2016.

Highly Sensitive Information Requires High Security, As These Databases May Be Frequent Targets

Breaches of Highly Sensitive Data

Year	Agency/Database	Number of Records	Method of Leak	Description
2011	Stratfor	3,300,000	Hacked	Members of the hacking collective known as "Anonymous" posted a file online of information from the Stratfor's confidential client list, containing passwords, home addresses and credit card details.
2012	Three Iranian Banks	3,000,000	Hacked	A hacker warned CEOs of Iran's banking system of a security vulnerability, yet his warnings went ignored. The hacker published card numbers and PINs of 3 million accounts to a website to prove the system's vulnerability.
2014	Korea Credit Bureau	20,000,000	Inside Job	An employee from the personal credit ratings firm was arrested for stealing the data from customers while working as a temporary consultant. The data included social security numbers, credit card numbers and names of what is estimated at almost half of the country's population.
2015	Internal Revenue Service (IRS)	100,0000	Poor Security	An unnamed cybermafia utilized the IRS website to download tax forms full of personal information. They attempted to download 200,000 forms, received 100,000 and were able to claim 15,000 tax refunds in other people's names.

Sources: Nicole Perlroth, "Questions About Motives Behind Stratfor Hack," The New York Times, December 27, 2011; AFP, "20 Million People Fall Victim to South Korea Data Leak," Security Week, January 19, 2014; Emil Protalinski, "3 Million Bank Accounts Hacked in Iran," ZDNet, April 16, 2012; Jose Pagliery, "Criminals use IRS website to steal data on 104,000 people," CNNMoney, May 26, 2015. Table is Excerpt from: David McCandless, "World's Biggest Data Breaches," Information Is Beautiful.net, February 16, 2016.

A Single Data Breach Could Affect Tens of Millions of People

Exceptionally Large Data Breaches

Year	Agency/Database	Number of Records	Method of Leak	Description
2007	TJ Maxx	94,000,000	Hacked	Hackers connected to a Minnesota store wifi network and stole data from credit and debit cards of shoppers from nearly 2,500 stores
2013	Court Ventures	200,000,000	Inside Job	A man posing as a private investigator from Singapore was allowed access to a personal records database by Court Ventures. He then ran a business of selling personally identifiable information to cybercriminals.
2013	Adobe	150,000,000	Hacked	Hackers retrieved data including customer names, encrypted credit/debit card numbers, passwords among other personal information and later posted the breached records onto a website frequented by cyber criminals.
2015	Target	70,000,000	Hacked	Hackers were able to obtain names, address, phone numbers and emails from shoppers at the retailer by hacking point-of-sale terminals at cash registers. The thieves also lifted an estimated 40,000,000 credit card records during the 2015 holiday shopping season.

Sources: Mark Jewell, "TJ Maxx Theft Believed Largest Hack Ever," NBC News, March 30, 2007; Sarah Perez, "Target's Data breach Gets Worse: 70 Million Customers Had Info Stolen, Including Names, Emails and Phones," TechCrunch, January 10, 2014; Chris Welch, "Over 150 million breached records from Adobe hack have surfaced online," Adobe, November 7, 2013. Table is Excerpt from: David McCandless, "World's Biggest Data Breaches," Information Is Beautiful.net, February 16, 2016.