The Edward Snowden NSA Data Breach of 2013: How it happened, and its consequences and implications for the U.S. and the IT Industry

William Favre Slater, III, M.S. MBA, PMP, CISSP, CISA Adjunct Professor, IIT School of Applied Technology
A Presentation for Forenssecure 2014
April 2014
WAKE UP AMERICA

"In the end the Obama administration is not afraid of whistleblowers like me, Bradley Manning or Thomas Drake. We are stateless, imprisoned and powerless. No the Obama administration is afraid of you. It is afraid of an informed, angry public demanding the constitutional government it was promised - and it should be."

Edward Joseph Snowden

Politifake.org

Edward Snowden’s Christmas Message to America, December 2013
Agenda

• Introduction
• What Happened? What Did Edward Snowden Do?
• How did he accomplish this?
• What has he disclosed?
• Consequences: How does this affect the NSA and U.S. National Security?
• Consequences: How will the Edward Snowden Compromise affect the U.S. Government?
• Consequences: Has anyone lost their job as a result of what Edward Snowden has done?
• Implications: How will the Edward Snowden Compromise affect the Cybersecurity Career Field
• Implications: How will the Edward Snowden Compromise affect your career?
• Implications: How would you prevent ant Edward Snowden-style Data Breach in your organization if your were the Cybersecurity Director?
• The Latest Developments on Edward Snowden
• Opinion: Do you think Edward Snowden was correct in doing what he did?
• Conclusion
• References
• Questions
Introduction

• The Edward Snowden 2013 NSA Data Breach was arguably the most damaging (known) data breach to ever impact the U.S. Intelligence Community. This presentation will cover what happened, how it happened, why it happened, the data breach’s consequences, its implications for the future, and how such breaches can be prevented in the future.
Some Previous Bad Security Breaches

A BRIEF HISTORY OF TOP SECURITY BREACHES

Data security has been a concern since the dawn of the spoken word, and breaches throughout history have led to both good and bad results for society. Today, with our information being mostly digital, hacks have become even more common. Employment of information security analysts, web developers and computer network architects is projected to grow 22% from 2010 to 2020¹ — faster than the average for all occupations. So, when did these data breaks begin? Here are some of history’s top information breaches.

1600
THE GUNPOWDER PLOT
November 5, 1605
A scheme to kill King James I using 36 barrels of gunpowder that Guy Fawkes was guarding was uncovered.

1700
CASANOVA
Spies for Venetian Inquisitors 1774–1783
Casanova spied for the Venetian Inquisitors of State.

1800
THE ENIGMA MACHINE
December 1932
Polish Cipher Bureau
The Polish government’s cryptography agency decoded the cipher for Germany’s early Enigma machines.

1900
WEST POINT SECRETS
April—September 1780
Benedict Arnold attempts to sell secrets to the British about American troops and West Point.
Some Previous Bad Security Breaches
Persons in the Story

Laura Poitras, Reporter

Barack Obama, President of the United States

Edward J. Snowden, Former NSA Contractor

Glen Greenwald, Reporter for the U.K. Guardian

Vladimir Putin, President of Russia

General Keith Alexander, Former NSA Director and Director of US Cyber Command

April 10, 2014

The Edward Snowden NSA Data Breach of 2013 by William Favre Slater III - Forensecure 2014
What Happened? What Did Snowden Do?

- In May 2013, after a series of secret communications with two experienced reporters (Laura Poitras and Glenn Greenwald), NSA Contractor and System Administrator Edward Snowden took four laptops, each with a 1 TB drive and flew to Hong Kong and later sought asylum in Russia.
- Approximately 1.7 million classified documents have been copied and removed from the NSA’s infrastructure while Snowden was on duty in Hawaii.
- The damage to the National Security of the United States is said to be “incalculable” and the WORST DATA BREACH EVER.
The Time Line

- **June 21, 1983** – Edward J. Snowden born in Elizabeth City, North Carolina
- **1999** – Dropped out of High School
- **2004** – Joined the U.S. Army Reserve because he was patriotic, later washed out
- **2005** - worked as a "security specialist" at the University of Maryland's Center for Advanced Study of Language
- **2006 - 2007** - Joined the CIA and worked as a system administrator in Geneva, Switzerland
- **2009** - Became a contractor and worked at Dell for the NSA in Japan
- **2012** - Was identified as having downloaded several sensitive documents from the NSA
- **January 2013** – Snowden initiates communications with a New York Times Reporter, Laura Poitras, setting the protocol for strong public key / private key encryption due to fears of being discovered
- **March 2013** – Snowden joined Booz Allen Hamilton as a systems administrator working for the NSA; moved to Hawaii
- **May 2013** – Snowden traveled from Hawaii to Hong Kong with Four Laptops; Meets Glenn Greenwald and Laura Poitras in Hong Kong
- **June 3 – 5, 2013** – Glen Greenwald published a series of articles in the U.K.’s Guardian newspaper disclosing the extent of the NSA’s surveillance programs, both foreign and domestic spying
- **June 21, 2013** – At the request of President Barack Obama, the U.S. Department of Justice files (sealed) criminal espionage charges against Snowden and demands extradition
- **August 1, 2013** – Snowden granted temporary political asylum in Russia by President Vladimir Putin after spending more than four weeks at the Moscow International Airport
- **March 7, 2014** - Testimony at EU Parliament via teleconference, e-mail, Twitter, and the Internet
- **March 10, 2014** – SXSW Conference via ACLU sponsored teleconference, Twitter, and the Internet
- **March 18, 2014** – the ACLU published all NSA documents that Snowden had disclosed so far, in an online database that is searchable by topic, title and date. The URL: [https://www.aclu.org/nsa-documents-search](https://www.aclu.org/nsa-documents-search)
- **March 18, 2014** – TED Conference Talk via Telepresence Robot, software and the Internet
- **April 6, 2014** – ACLU Conference via teleconference, e-mail, Twitter, and the Internet
- **April 8, 2014** – Edward Snowden Interview in Vanity Fair magazine
How Did Snowden Accomplish His Data Breach?

• Social Engineering
  – Achieved Elevated Privileges and Access by getting colleagues to share their login credentials
  – Defeating security controls that were designed to compartmentalize data and data access based on a need to know
• Intimate knowledge of systems, security management, and weaknesses in controls
• Copied data to four Laptops – 1 TB each
• Communicated with Reporters starting in January 2013 via encrypted e-mails
• Left Hawaii to Hong Kong gave reporters key details
• Left Hong Kong for asylum in Russia
• Communicating now via the Internet (e-mail, secure webcast, Twitter, Telepresence Robot control, phone, etc.)
What Has Snowden Disclosed?

• Details about
  – MANY NSA Classified Programs
  – MANY GCHQ Classified Joint Programs
  – Spying on Americans
  – Spying on Allies
  – Spying on our “Enemies”
  – Social Engineering and Discrediting Campaign Tactics
  – NSA working Microsoft, Google, Yahoo. Etc.
  – Offensive and Defensive Cyberwarfare activities and actors
  – Workings of the NSA and his job responsibilities
  – His philosophies and believes about the Government, surveillance, the Internet, and personal freedoms

• Promises to disclose a great deal more
NSA Surveillance Programs – Now Known

Pre-2001
ECHELON
Main Core
MINARET
SHAMROCK
PROMIS

Since 2001
BLARNEY
RAGTIME
Turbulence
PINWALE
MAINWAY
Upstream

Since 2007
PRISM
Boundless Informant
X-Keyscore
Dropmire
Fairview Surveillance Detection Unit
Bullrun
MYSTIC
Tubine
Quantumhand
Synapse

GCHQ collaboration
MUSCULAR
IMP
JTRIG
Tempora
Mastering the Internet
Global Telecoms Exploitation

Discontinued
Trailblazer
Project ThinThread
President’s Surveillance Program
Terrorist Surveillance Program
 STELLARWIND

Disclosed in Detail by Snowden
Current Efforts - Google

GFE = Google Front End Server
SSL Added and removed here!
Traffic in clear text here.

Gmail Docs
Maps
DC
DC
DC

PUBLIC INTERNET
GOOGLE CLOUD

TOP SECRET//SI//NOFORN
INTRODUCTION
US as World Telecommunications Backbone

- Much of the world’s communications flow through the US.

- A target’s email, phone call or chat will take the cheapest path, not the physically most direct path— you can’t always predict the path.

- Your target’s communications could easily be flowing into and through the US.
PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- Special Requests

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN
Dates When PRISM Collection Began For Each Provider

- Microsoft: 3/12/07
- Yahoo: 6/3/09
- Facebook: 12/7/09
- PalTalk: 9/4/10
- YouTube: 2/6/11
- Skype: 3/31/11
- AOL: 3/31/11
- Apple: (added Oct 2012)

PRISM Program Cost: ~ $20M per year
• Set up a honey-trap
• Change their photos on social networking sites
• Write a blog purporting to be one of their victims
• Email/text their colleagues, neighbours, friends etc
Discredit a company

- Leak confidential information to companies / the press via blogs etc
- Post negative information on appropriate forums
- Stop deals / ruin business relationships

TOP SECRET\COMINT\REL TO USA, AUS, CAN, GBR, NZL
## Gambits for Deception

<table>
<thead>
<tr>
<th>Attention</th>
<th>Perception</th>
<th>Sensemaking</th>
<th>Affect</th>
<th>Behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control attention</td>
<td>Mask/Mimic</td>
<td>Exploit prior beliefs</td>
<td>Create Cognitive Stress</td>
<td>Simulate the action</td>
</tr>
<tr>
<td>Conspicuity &amp; Expectancies</td>
<td>Eliminate - Blend</td>
<td>Present story fragments</td>
<td>Create Physiological Stress</td>
<td>Simulate the outcome</td>
</tr>
<tr>
<td>The big move covers the little move</td>
<td>Repackage/Invent</td>
<td>Repetition creates expectancies</td>
<td>Create Affective Stress (+/-)</td>
<td>Time-shift perceived behaviour</td>
</tr>
<tr>
<td>The Target looks where you look</td>
<td>Dazzle/Decoy</td>
<td>Haversack Ruse (The Piece of Bad Luck)</td>
<td>Cialdini+2</td>
<td>Divorce behaviour from outcome</td>
</tr>
<tr>
<td>Attention drops at the perceived end</td>
<td>Make the cue dynamic</td>
<td>Swap the real for the false, &amp; vice versa</td>
<td>Exploit shared affect</td>
<td>Channel behaviour</td>
</tr>
<tr>
<td>Repetition reduces vigilance</td>
<td>Stimulate multiple sensors</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SECRET//S//REL TO USA, FVEY
Consequences: How does this affect the NSA and U.S. National Security?

• One U.S. Government Official:
  – “We have to assume that the Russians know EVERYTHING about our Surveillance Programs…”
• The U.S. will have to go back to the drawing board to create and implement most of the programs that provided the capabilities they want and need
• The NSA and other Intelligence gathering agencies must now rethink their human security programs
• Fewer people will have access to highly classified data
Consequences: How will the Edward Snowden Compromise affect the U.S. Government?

• Better Risk Assessment and Risk Management Programs
• Better security management
• More money will be spent creating new surveillance programs and data protection programs
• Fewer people will have access to highly classified data
• Those with access to data will be watched more carefully
• Quicker and Harsher punishment for infractions
(Sealed) Charges Filed Against Edward Snowden

• June 21, 2013 – the U.S. Filed Criminal Charges Against Former NSA Contractor, Edward Snowden

• If convicted, Snowden could get the death penalty
April 10, 2014
The Edward Snowden NSA Data Breach of 2013 by William Favre Slater III - Forensecure 2014

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

United States of America
v.
Edward J. Snowden

(v/indict(s))

Case No: 1:13 CR 266 (CMH)

UNDER SEAL

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 2013 in the county of Not Applicable in the

District of Not Applicable, the defendant(s) violated:

Code Section Offense Description
18 U.S.C. 641 Theft of Government Property
18 U.S.C. 793(d) Unauthorized Communication of National Defense Information
18 U.S.C. 796(a)(3) Willful Communication of Classified Communications Intelligence Information to an Unauthorized Person

This criminal complaint is based on these facts:
See Attached Affidavit.
Venue is proper pursuant to 18 U.S.C. 3238.

Continued on the attached sheet.

Reviewed by AUSA/SAUSA:

Sworn to before me and signed in my presence.

Date: 06/14/2013

City and state: Alexandria, VA

John F. Anderson
United States Magistrate Judge

Hon. John F. Anderson, U.S. Magistrate Judge

Illinois Institute of Technology
Consequences: Has anyone lost their job as a result of what Edward Snowden has done?

- General Keith Alexander, chief of the NSA, Central Security Service, and U.S. Cyber Command AND his Deputy John Inglis
  - On October 16, 2013, it was announced that General Alexander, and his Deputy John C. Inglis, were leaving the NSA. This announcement came on the heels of four months of NSA spying revelations spawned by press-leaks made by former NSA contractor Edward Snowden.

- Most likely some of Snowden’s bosses at the NSA and Booz Allen Hamilton were quietly fired
Implications: How will the Edward Snowden Compromise affect the Cybersecurity Career Field

• More qualifications and experience
• More frequent training
• More certifications
• More stringent controls
  – More surveillance
  – Background checks
  – Better control of access to data
  – Two-man policies

April 10, 2014

The Edward Snowden NSA Data Breach of 2013 by William Favre Slater III - Forensicure 2014
Implications: How will the Edward Snowden Compromise affect your career as an IT Professional?

• The qualifications bar will be much higher
  – No more high school drop-outs or GEDs
  – More certifications, cybersecurity-related degrees

• Stronger examination of backgrounds

• Expect more oversight
Implications: How would you prevent an Edward Snowden-style Data Breach in your organization if you were the Cybersecurity Director?

• Revamp your **Risk Assessment and Risk Management Programs**
• Revamp your **Security Management Program**
  – Applying the Control Framework(s) controls that relate to Security Personnel and Asset Management
  – Training on Security, ethics, etc.
  – Increased surveillance, controls and accountability
  – Fewer people should have access to highly classified data
  – Two-man policies
• Apply and use metrics
• Monitor! Monitor! Monitor!
• Continuously improve
• Train! Train! Train!

The Latest Developments on Edward Snowden

- **March 7, 2014** - Testimony at EU Parliament
- **March 11, 2014** – SXSW Conference
- **March 18, 2014** – TED Conference
- **April 6, 2014** – ACLU Conference
- Has promised to release MANY more revealing documents
- Has set up a “Doomsday” release arrangements of all documents in case he is assassinated
Edward Snowden’s 6 Revelations at the SXSW Conference

1. Bulk Data Collection Doesn't Work
2. There Isn't Much Consumers Can Do to Avoid It
3. The Most Dangerous Men in America Are Michael Hayden and Keith Alexander
4. The Government Still Doesn't Know What Snowden Has
5. The Tech Industry Is Upset
6. Snowden Has No Regrets

"The NSA is setting fire to the Internet. You people in the room at SXSW are the firefighters." – Edward Snowden

6 Things Edward Snowden Revealed at SXSW
http://www.pcmag.com/article2/0,2817,2454827,00.asp
The EU Parliament in a show of Solidarity for Edward Snowden and his disclosures votes in support of anti-spying measures
Opinion: Do you think Edward Snowden was correct in doing what he did?

- Let’s take a vote using a show of hands

<table>
<thead>
<tr>
<th>Snowden was WRONG</th>
<th>Snowden was RIGHT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Anecdotal Advice to Prevent an Edward Snowden Event in your Organization:

1. Learn about vetting your people with background checks.
2. Learn about monitoring your peoples’ work and behaviors.
4. Learn about and train your system administrators on a Code of Ethics: http://1drv.ms/QjMcjw
5. Learn about and train your entire staff about what Social Engineering is, how it works, and how to protect against it.
6. Read this paper about Hacking Humans: http://www.billslater.com/writing/Hacking_Humans_from_W_F_Slater_v1_2013_0219_.pdf
Conclusions

- Despite billions of dollars of planning, engineering and administration, the human element proved to be the weakest link.
- A lot of security REENGINEERING will need to take place.
- A lot of money, time, and energy will be required to get it corrected.
- Things will get more complicated for Management and Cybersecurity professionals.
- Greater vetting efforts and compartmentalization of data.
- Expect that highly-trained, high-skilled, trustworthy cybersecurity professionals and managers will be more valuable and in demand.
The End... of The Beginning

The Brand New 1 million square foot NSA Data Center in Bluffdale, Utah
This 100 MW Facility will hold 12 Exabytes of Data

It houses EVERYONE’s Data
References

- New Books on Edward Snowden

- No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State
- The Snowden Operation: Inside the West’s Greatest Intelligence Disaster
- No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State
References


References


References


References

Questions?
Career Opportunities?

- Yes – The U.S. Government is hiring Cybersecurity Professionals
- Private Industry will be picking up more and more Cybersecurity experts

U.S. Federal Cybersecurity Market
$65.5 Billion in 2013-2018
CAGR 6.2%
Career Development Opportunities?

Illinois Institute of Technology
• M.S. in Cyber Forensics and Security (land campus)

Bellevue University
Bellevue, NE (land campus and online)
• M.S. in Cybersecurity
• B.S. in Cybersecurity

http://www.itm.iit.edu/cybersecurity/index.php

http://www.bellevue.edu/degrees/graduate/cybersecurity-ms/

April 10, 2014
The Edward Snowden NSA Data Breach of 2013 by William Favre Slater III - Forenssecure 2014
Presenter Bio: William Favre Slater, III

- IT professional since July 1977
- Owner of Slater Technologies, Inc.
- An Adjunct Professor at the Illinois Institute of Technology – for six years
- first Data Center Manager of Microsoft’s Flagship Cloud Data Center, the Microsoft Chicago Data Center in 2008
- Managed Data Centers at BP from August 2001 – November 2006, was also a Change Management Manager and a System Administrator during that time.
- Have achieved 80 IT-related certifications, including PMP, CDCP, CISSP, SSCP, CISA, MCITP, MS Project, Visio, MCSE 2003 Security & Messaging, MCSD, MCAD, MCDST, and MCT
- Data Center Technology Program – Marist College & the Institute of Data Center Professionals, February 2008 – Received the Certified Data Center Professional Certification
- M.S. in Cybersecurity – Bellevue University, Bellevue, NE (completed on March 2, 2013)
- MBA, University of Phoenix, 2010
- MS in Computer Information Systems, University of Phoenix, 2004
- BS in Engineering Technology with a major in Computer Systems Technology, University of Memphis
- Published author & editor: Magazines, books, courseware
- Subject Matter Expert in Cybersecurity for Caveon Courseware and Testing
- Happily married (since December 2000) to Joanna K. Roguska, who is a professional web developer
- A former U.S. Air Force computer systems staff officer at Strategic Air Command Headquarters supporting the SAC Underground and SAC Battle Staff Command Control Communications Systems, July 1977 – October 1980
- Native of Memphis, Tennessee, born the same month and year as Bill Gates
- Resident of Chicago
- Active member of Chicago Police Judo Club and a Black belt in Kodokan Judo, since 1988
Presenter Bio:
William Favre Slater, III

- **Current Position** – Project Manager / Sr. IT Consultant at Slater Technologies, Inc. Working on projects related to
  - Security reviews and auditing
  - ISO 27001 Project Implementations
  - Subject Matter Expert for preparing Risk Management and Security Exams at Western Governor’s State University in UT
  - Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
  - Providing subject matter expert services to Data Center product vendors and other local businesses.
  - Developing and presenting technical training materials for undergraduate and graduate students at the Illinois Institute of Technology in the areas of Data Center Operations, Data Center Architecture, Cyber Security Management, and Information Technology hardware and software.