Cyber Security Month 2019
Basic Cyber Security Concepts

CSUF CYBERSECURTIY SYMPOSIUM

Jason G. Weiss, Counsel

Information Governance & Electronic Discovery Group

- Los Angeles Office
- Drinker Biddle & Reath
- 310-203-4062
- Jason.Weiss@DBR.com

DrinkerBiddle®

This presentation is for informational purposes only. The material contained herein is general and is not intended to be legal advice. It should not be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Law Enforcement Background (22 years)

- Joined the FBI in May of 1997 – completed 17 weeks at FBI Academy in Quantico, VA
- First Office Agent in San Diego, CA (1997) – originally handled Violent Crime, Bank Robberies, Applicants and White Collar Crime; Assigned to Los Angeles Field Office May 2003
- In July of 1998 Assigned to first ever San Diego Cyber Crime Squad where worked computer intrusions and crimes against children; Shortly after assigned to the FBI San Diego Cyber Squad in 1998 moved to blended mission of cyber and computer forensics

Cyber Security Experience

- Worked scores of Cyber Forensics cases covering all aspects of cyber crime over FBI career including numerous cyber breach cases – both criminal and national security
- Developed a highly-secure system for enabling information-sharing between FBI and private sector partners, which now serves as a gold-standard model the FBI.
- Developed an FBI Cyber Task Force national pilot program to coordinate the sharing of critical cyber threat information among private sector, academia, financial institutions, universities and port authorities. Created platform used to facilitate an unprecedented level of partner information sharing, thus mitigating and neutralizing cyber threats from hackers and hostile foreign adversaries.
- Certified as an FBI Adjunct Instructor in the Cyber Field Instructor Program and taught cyber seminars both domestically and internationally

Computer Forensics Experience

- Worked approximately 700 cases as an FBI Senior Computer Forensic Examiner, including over 100 Cyber cases and over 50 mobile forensic exploitation cases
- Spent 21 years in the FBI's Computer Forensics Program and created a nationally recognized forensic laboratory and served as the founding Laboratory Director and Task Force Commander. Transformed the local FBI program into a Regional Task Force serving over 200 law enforcement agencies in Southern California
- Helped created FBI-wide policies to maintain forensic evidence, including how to identify, seize, and preserve all forms of digital data while ensuring all Attorney General Guidelines are met, serving as a model for all national FBI forensic programs

Teaching and Training Experience

- Teaching and training have been a central element of distinguished career in law enforcement, computer forensics, cybersecurity, and as an attorney. As a teacher and instructor, he has both developed and delivered dozens of professional certification and training courses as well as courses at postsecondary and graduate institutions
- Teaching and training topics include digital evidence and the law; electronic discovery; computer forensics lab design and development, computer forensics lab accreditation; digital evidence identification, seizure and collection; transitive digital evidence; data breach response and intrusion detection. Taught over 50 Cyber and Forensics Courses domestically and internationally (Philippines, Nigeria, Bangladesh, Ukraine, Ghana and Indonesia)
- Been an FBI Adjunct Instructor since 2002, teaching Digital Evidence Identification, Collection and Seizure to over 1000 FBI Evidence Response Team Members. Certified by the FBI to teach in the Cyber Field Instruction Program, Forensic Digital Evidence, Digital Science and Forensics and Digital Evidence Extraction

CYBERSECURITY CONCEPTS

What is Cyber Security?

- Cyber Security is the protection of data and systems within networks that are connected to the Internet, including:
  - Information Security
  - Information Technology Disaster Recovery
  - Information Privacy
- In short, Cyber Security means different things to different people depending on your:
  - Job Title (C-Suite v. IT Manager, etc)
  - Job Position and Responsibilities
  - What you are required to protect on a computer network

What is Cyber Security?

- There are two main type of Cyber Security "defenses" to be aware of:
  - Technical Defense Techniques
  - Social Awareness Techniques
- Both of these defenses are important but for different reasons:
  - Your technical defense provides actual network and machine security through the use of firewalls, routers, and many other traditional IT security defenses
  - Your Social Awareness defenses may, however be the most important of all – it trains everyone in your company on how to avoid being subject to a successful cyber attack

What is Cyber Social Awareness Training?

- Most companies have very astute IT departments to keep their hardware and their networks safe….
  - There is not time here to discuss all the intricacies of technical IT defense, so I want to discuss the REALLY IMPORTANT way to defend your data….
- Which leads to the most critical question of the day:
  - What is the **WEAKEST** part of any organization’s data security plan?

Protecting Your Network & Your Data

- The weakest security part of any business are the

EMPLOYEES

- The FBI had a saying they would drum into us almost daily → The only safe network is a network with no users!

What is Social Engineering?

- Social Engineering is the term used for a BROAD range of malicious activities accomplished through simple human interaction and a fair share of "trickery"
- Social Engineering uses "psychological manipulation" to basically trick employees into making security mistakes or giving away sensitive information

How Does Social Engineering Work?

- Social Engineering is a multi-faceted attack and includes:
  - The perpetrator first investigates the intended victim gather necessary background information, such as potential points of entry and weak security protocol needed to proceed with the attack
  - The attacker then moves to gain the victim’s trust and provides a stimuli for subsequent action that breaks established security practices, such as revealing sensitive information and granting access to critical resources (www.imperva.com)
- Social Engineering is simply the most efficient, cost effective and capable tool used by cyber-criminals in so many different types of crimes
  - The original master of social engineering was one of the most famous hackers our generation, Kevin Mitnick. They have literally written books about him and how he used social engineering to effectuate his attacks

Common Social Engineering Attacks

Attack Type	What Happens in the Attack
Phishing	Targeting people through social media ruse
Spear Phishing	Targeting specific group of people
Whaling	Targeting business execs
Watering Hole	Injecting malicious script in public websites
Pretexting	Faking your identity
Tailgating	Piggy backing into a restricted site
Dumpster Diving	Going through garbage bins for sensitive info
Quid Pro Quo	Hacker offers service in benefit for an exchange
Business E-mail Compromises (BEC)	Faking fraudulent wire transfers - BEC has become the single largest damages claim today for Cyber Insurance

Common Social Engineering Attacks

- Cyber Social Engineering can lead to many different problems for any business, financial and otherwise:
    - RANSOMWARE
    - MALWARE
    - BUSINESS EMAIL COMPROMISE
    - ECONOMIC ESPIONAGE
    - LOST DATA
    - DATA SNIFFERS
    - KEYBOARD STROKE MONITORS
    - THEFT OF E-MAIL
    - THEFT OF INTELLECTUAL PROPERTY
    - EXORBITANT COSTS TO SECURE NETWORK

WHY IS THIS IMPORTANT

Basic Numbers to Consider with Cyber Security

- In 2019 Alone:
  - Average cost of cybercrime (for a large company) has risen significantly over the last year alone:
    - The average annual cost has increased over 1.4 million dollars to 13 million dollars a year in lost costs
    - Number of security breaches for the average organization rose by 11% from approximately 130 to 145 attacks per year

- Overall the numbers are much scarier (2005-2014):
  - In 2014 there were 783 data breaches reported, with at least 85 million total records exposed and stolen representing an increase of over 500 percent from 2005

Basic Numbers to Consider with Cyber Security

- More numbers to consider:
  - It is estimated that malicious cyber attacks cost the US economy between $57 billion and $109 billion in 2016 alone

- The current numbers for 2019 are staggering:
  - IN 2019 to date there have been more than 4800 data breaches just REPORTED alone
  - This is a 50% increase over the last 4 years alone – some have estimated that the actual number is close to a 55% increase in breaches

Basic Numbers to Consider with Cyber Security

- Some of the more well known and expesive hacks over just the last few years alone:
- Some of these well known breaches over the last few years include, but are not limited to:
  - Marriott Breach (2018) – 500 Million Accounts compromised***
  - Equifax Breach (2017) – 143 Million Accounts compromised
  - Adult Friend Finder (2016) - 412 Million Accounts compromised
  - Anthem (2015) – 78.8 Million Accounts compromised
  - E-Bay (2014) – 145 Million Accounts compromised
  - JP Morgan Chase (2014) – 76 Million Accounts compromised
  - Home Depot (2014) – 56 Million Accounts compromised
  - Yahoo (2013) – Approximately 3 Billion accounts compromised
  - Target Stores (2013) – 110 Million Accounts compromised
  - Adobe (2013) – 38 Million Accounts compromised

QUESTIONS???