Cyber Terrorism or Data Breach? A New Role for Victim Services

September 10, 2015
1:30 pm
Overview

• What is cyber crime & what types exist?
• What unique challenges are present when large data breaches occur?
• What are the effects on victims – emotionally & in terms of compromised identity or security?
• How can victim serving professionals assist in recovery & minimizing re-victimization?
• What resources exist to learn more & get involved?
Presenters

• Laura Ivkovich, DOJ - Office for Victims of Crime
• Michael Kaiser, National Cyber Security Alliance
• Terri Howard, FEI Behavioral Health
• Merry O’Brien, National ID Theft Victim Assistance Network
Cyber Crimes:

Basic Categories

Criminal Motivations

Challenges in Assisting Victims of Data Breaches
Who are the Attackers & What are their Motivations

- **Who**: Cybercriminals
- **Why**: Money
- **Types of attacks (generally)**:
  - Retail data breaches
    - Target, Home Depot, POS systems, healthcare records
  - Phishing attacks via email, texts, social posts, or any system that can yield data that can be monetized.
Who are the Attackers & What are their Motivations

• **Who:** Nation States
• **Why:** Intelligence, Disruption
• **Types of attacks (generally):**
  – Data collection/stealing IP (OPM, Anthem) and/or disruption (Saudi Aramco, Sony)
  – Attacks on infrastructure like wall street, transportation, electric grid, water systems, etc.
Who are the Attackers & What are their Motivations

- **Who**: Hacktivists (like Anonymous):
- **Why**: Disruption, Embarrassment, Justice seeking

**Types of attacks (generally):**
- Disruption (Targeting police departments after events like Ferguson)
- Embarrassment (Ashley Madison, Sony) and/or
- Justice seeking (Steubenville, OH)
Example of Justice Seeking

On December 24, 2012, the hacker collective Anonymous threatened to reveal the names of other unindicted alleged participants.

In December 2012, KnightSec, an offshoot of Anonymous, hacked an unaffiliated website, posting a demand for an apology by school officials and local authorities, who had allegedly covered up the incident in order to protect the athletes and school's program.

KnightSec followed up their December hack on January 1, 2013, posting a video featuring the "self-proclaimed 'rape crew' from the night of the attack, making jokes about what had happened."
How Do Cyber Crime Victimizations Occur?

- Data breaches, hacking into computers and networks at health care agencies, businesses, or schools that have information
- Phony emails from imposters
- Unsecure Wi-Fi hotspots
- Peer-to-peer file sharing
- Social networking
- Downloading software or apps from unknown sources
- Password cracking
- Malvertising
- Infecting devices
Risks to Victims

- **Cybercriminals**: Financial loss, identity theft, privacy violations.
- **Nation States**: Financial loss (if data is sold) or IP stolen, privacy violations/security issues (OPM/Sony), attacks on critical infrastructure leading to communitywide issues (loss of services, etc)
- **Hacktivists**: Additional emotional pain, privacy violations, including breaching of confidentiality, disrupting or biasing a court proceeding.
Breaches Can Lead to ID Theft

Misuse of another’s PII:
- Name, address, number, DOB, SSN, Driver’s License
- Medical: Medicare or health insurance number
- Financial: bank account, credit card numbers
- Passwords (maiden names, etc.)
- Biometric data (fingerprint, iris scan)

In order to:
- fraudulently obtain goods, services, job, benefits, medical
- hide from government, law enforcement, others who perform background checks
Victim Impact

- Emotional
- Personal Security
- Compromised PII
Impact & Response Trauma

- Stressful

- Outside normal range of experience

- Usual coping mechanisms are insufficient

- Threatens to or actually causes psychological destabilization

- May include intense physical and/or psychological suffering

- No warning or time for preparation
Emotional Reactions

- Feeling of anxiety of helplessness
- Anger
- Irritability
- Guilt (self-blame)
- Vulnerability
- Isolation
- Mistrustful
- Violated
Behavioral Reactions

- Difficulty concentration
- Insomnia
- Loss of appetite
- Loss of interest in activities/work
- Absenteeism
- Lack of focus
Physical Reactions

Heart palpitations
Sweating
Constipation/diarrhea
Aches and pains
Effects of Compromised PII

- Reduced ability to escape a domestic violence abuser or stalker
- Direct financial loss, damage to credit score, reputation
- Denial of employment, housing
- Problems with IRS
- Civil judgments, criminal record, false arrest
- Emotional harm
- Time and cost of repairing damage
“Captain Michael Gorhum of San Antonio PD took his life after his official email address was published on a list of purported Ashley Madison users. But his email is not in actual Ashley Madison leak.”
Sony Hack Identity Theft Victim: I Can't Find a Job Now

Freelance film accountant Nicole Basile's name was used in emails sent by hackers pointing journalists to stolen files, after which she was flooded with calls, texts and emails.

This story first appeared in the Jan. 9 issue of The Hollywood Reporter magazine.

Freelance film accountant Nicole Basile's phone began buzzing nonstop Dec. 3 with calls, texts and emails from family, friends and reporters. With no warning, the 31-year-old...
Fed charged with 'sextortion,' cyberstalking from US embassy

A State Department employee at the U.S. Embassy in London was indicted this week for allegedly stealing hundreds of women's passwords, breaking into their email and social media and using sexually graphic photos and other sensitive information to extort them.

While working out of the London offices, Michael Ford, 36, allegedly used several pseudonyms while posing as an employee of an email service provider to reach out to hundreds of women and threaten to shut down their accounts unless they sent him their passwords.

Related: Former fed charged in spear-phishing attempt on colleagues

Once he had the passwords, Ford was able to access the victims' email and social media accounts to steal revealing photos and personal information. With that information, he allegedly blackmailed the victims, threatening to release the photos and information unless they sent him "videos of 'sexy girls' undressing in changing rooms at pools, gyms and clothing stores," according to the indictment.
When ID Theft Occurs

- $1,870 average out-of-pocket for recovery
- Over 3 million experienced issues such as having utilities cut off, being arrested, finding erroneous claims on their health records, having child support garnished for children they never had, and being harassed by collection agencies

Bureau of Justice Statistics Special Report, National Crime Victim Victimization Survey Supplement
Not a “Victimless Crime”
Victim Assistance

Recovery

Minimizing Re-Victimization
Advocacy Skills

• LISTEN
  • You may be the first person to listen to what the victim is experiencing and feeling

• DON’T JUDGE the victim
  – A lot of well meaning people have a tendency to blame the victim, when it’s not the fault of the victim

• NORMALIZE feelings
  – Explaining that many victims of these crimes feel this way
Basic Strategy

- Stop the activity
- Report the crime
- Repair the damage
- Prepare for re-victimization
Accessing the Damage & Reporting

• Help victim contact credit reporting agencies
  – place a fraud alert
  – determine if a credit freeze may be useful
  – request/review credit report

• Help victim file a complaint with the FTC at 877-ID-THEFT

• Encourage victim to file a police report (optional, although helps victim assert rights)

• Help victim contact companies where fraud occurred
Fraud Alerts

• 90 days & Renewable for 7 years
• Entitles victim to one additional, free credit report
• Need to call only one of the credit reporting agencies; it will notify the others.
• Creditors must take “reasonable steps” to verify one’s identity

Credit Freezes

• Effective until lifted
• Must request in writing from each credit reporting agency
• Blocks all new credit
Prevention &
How To Lessen Your Client’s Chance of Re-Victimization
How to Help Victims

• Educate victims on online safety & security basics: keep a clean machine, get two steps ahead, share with care, etc.

• Help the assess risks after data loss to enact specific steps by focusing on specifics of each case.

• Teach them to engage in ongoing evaluation of the threat, such as checking credit & statements.
Educate Your Clients

- Minimize PII in wallets or phones & keep PII secure ..home/office/car
- Help clients become more aware of risks of personal information through use of workplace computers
- Don’t click on links sent in unsolicited email
- Monitor accounts & review financial statements regularly
- Watch mail for statements for unknown accounts or credit cards
- Free annual credit report: www.annualcreditreport.com
- Copy everything in wallet & store it safely
- Sign up for BBB scam watcher: www.bbb.org/council/bbb-scamm-stopper
- Register with FTC’s Do-Not-Call Registry: 1-888-382-1222 or donotcall.gov.
- Opt out of credit offers - 1-888-5-OPTOUT or optoutprescreen.com
- Use Facebook security settings
Resources

National Resources

Awareness Campaigns
• State Victim Resources (numbers, links)
• Laws including Civil Suits, Access Devices, Cyber Crimes, Security Breaches
• Security Freeze Law & State-Specific How To’s
• Mandatory Police Report Law for IDT Victims
• ID Theft Passport Law
• Inclusion in state’s restitution definitions

ovcttac.gov/identitytheftnetwork
Twitter.com/IDTheftNetwork
Facebook.com/IdentityTheftNetwork
• Printable Outreach Material
  – Brochures
  – Website Material
  – PSA Scripts & Audio & Visual Samples
• Quick Tip Sheets
• Ready-To-Use Forms
• Sample MOU’s
• Training Slides, Instructor Manuals, Worksheets
Advocate’s Guide to Assisting Victims of Financial Fraud

www.saveandinvest.org

Taking Action

An Advocate’s Guide to Assisting Victims of Financial Fraud

Steps to Recovery for Victims:

STEP 1 – Place a Fraud Alert
The victim should first place a fraud alert with one of the three credit reporting companies in order to be notified of any fraudulent requests for credit. The victim will need to:

- contact one of the three credit reporting companies (Equifax, Experian, or TransUnion);
- tell the company he or she is a victim of an identity theft and request that a fraud alert be placed on his or her credit report (this initial fraud alert will last for 90 days);
- ask the company to report this request to the other two credit reporting companies; and
- order his or her free credit report (by creating the fraud alert, the victim is entitled to one free copy from each credit reporting company within 12 months of placing the alert).

CREDIT REPORTING COMPANIES
All consumers, regardless of a fraud alert, are entitled to receive one free credit report every 12 months from each of the following companies:

EQUIFAX
(800) 685-1111
www.equifax.com

EXPERIAN
(888) 397-3742
www.experian.com

TRANSUNION
(800) 916-8800
www.transunion.com

STEP 2 – Create an Identity Theft File
Victims should maintain one central file that contains all relevant documentation concerning the fraud. This file is for the victims to maintain only and should be kept in a secure location.
OVC - Online Interactive Training for Advocates
www.ovcttac.gov/IdentityTheft
Get Involved in Education & Awareness

• Have tip sheets and posters available at your offices on staying safe online, keeping kids safe & mobile - free at www.stopthinkconnect.org

• Participate in ongoing awareness events:
  – National Cybersecurity Awareness Month - October
  – Data Privacy Day - January 28th
  – Safer Internet Day – February 9th
  – National Consumer Protection Week - March
Website Round-Up

- **Stop. Think. Connect.** - stopthinkconnect.org & dhs.gov/stopthinkconnect
- **Stay Safe Online** - staysafeonline.org
- **On Guard Online** - onguardonline.gov
- **Better Business Bureau** - bbb.org
- **FTC** - identitytheft.gov
- **IRS** - irs.gov/identitytheft
- **Office for Victims of Crime** - ovc.gov
- **National ID Theft Victims Assistance Network** - identitytheftnetwork.org
- **AARP** - aarp.org/FraudWatchNetwork
- **Identity Theft Resource Center** - idtheftcenter.org
ITRC ID Theft Help Mobile App

The ID Theft Help app, which was funded by a grant from the Department of Justice, Office for Victims of Crime (OVC), helps consumers protect themselves against identity theft, completely free of charge.

Features:
• Identity Theft Q&A Solution Tree
• LiveChat
• Direct Dialing
• Educational Information
• Resources

The ITRC ID Theft Help Mobile App is available on both the Apple and Android Platforms and is completely free of charge.
Questions?

- **Laura Ivkovich**, DOJ, Office for Victims of Crime: laura.ivkovich@usdoj.gov
- **Terri Howard**, FEI Behavioral Health: thoward@feinet.com
- **Merry O’Brien**, National ID Theft Victim Assistance Network: info@identitytheftnetwork.org
- **Michael Kaiser**, National Cyber Security Alliance: michael@staysafeonline.org