Cyber Security for Pharma and Medical Device Companies

Thomas G.A. Brown, JD

Managing Director, Global Practice Leader – Cyber Security & Investigations, Berkeley Research Group; Former AUSA, U.S. Attorney's Office for the Southern District of New York; New York, NY

Justin Herring, JD

Assistant United States Attorney, United States Attorney's Office, District of New Jersey, US Department of Justice, Newark, NJ

William J. Hughes, Jr., JD, LLM

Principal, Porzio, Bromberg & Newman, PC; Assistant US Attorney and Trial Attorney, US Department of Justice, Morristown, NJ (Moderator)

BRG
Berkeley Research Group

PORZIO
BROMBERG&NEWMAN P.C.

2017 Data Breaches

The New York Times

MARCH 7, 2017

WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents

WASHINGTON — In what appears to be the largest leak of C.I.A documents in history, WikiLeaks released on Tuesday thousands of pages describing sophisticated software tools and techniques used by the agency to break into smartphones, computers and even Internet-connected televisions.

The documents amount to a detailed, highly technical catalog of tools. They include instructions for compromising a wide range of common computer tools for use in spying: the online calling service Skype; Wi-Fi networks; documents in PDF format; and even commercial antivirus programs of the kind used by millions of people to protect their computers.

2017 Data Breaches

MAY 12, 2017

The New York Times

Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool

SAN FRANCISCO — Hackers exploiting malicious software stolen from the National Security Agency executed damaging cyberattacks on Friday that hit dozens of countries worldwide, forcing Britain's public health system to send patients away, freezing computers at Russia's Interior Ministry and wreaking havoc on tens of thousands of computers elsewhere.

2017 Data Breaches

BRG Berkeley Research Group

PORZIO BROMBERG&NEWMAN P.C.

2017 Data Breaches

The New York Times

JUNE 22, 2017

A Cyberattack 'the World Isn't Ready For'

The strike on IDT, a conglomerate with headquarters in a nondescript gray building here with views of the Manhattan skyline 15 miles away, was similar to WannaCry in one way: Hackers locked up IDT data and demanded a ransom to unlock it.

But the ransom demand was just a smoke screen for a far more invasive attack that stole employee credentials. With those credentials in hand, hackers could have run free through the company's computer network, taking confidential information or destroying machines.

2017 Data Breaches

The New York Times

Sept. 7, 2017

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

Equifax, one of the three major consumer credit reporting agencies, said on Thursday that hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver's license numbers.

The attack on the company represents one of the largest risks to personally sensitive information in recent years, and is the third major cybersecurity threat for the agency since 2015.

Number Of Records Exposed From Reported Data Breaches in 2016

- 4,149 Reported Data Breaches
- 4.2 Billion Records
- MySpace & Yahoo Data Breaches Accounted for 2.2 Billion Records Compromised

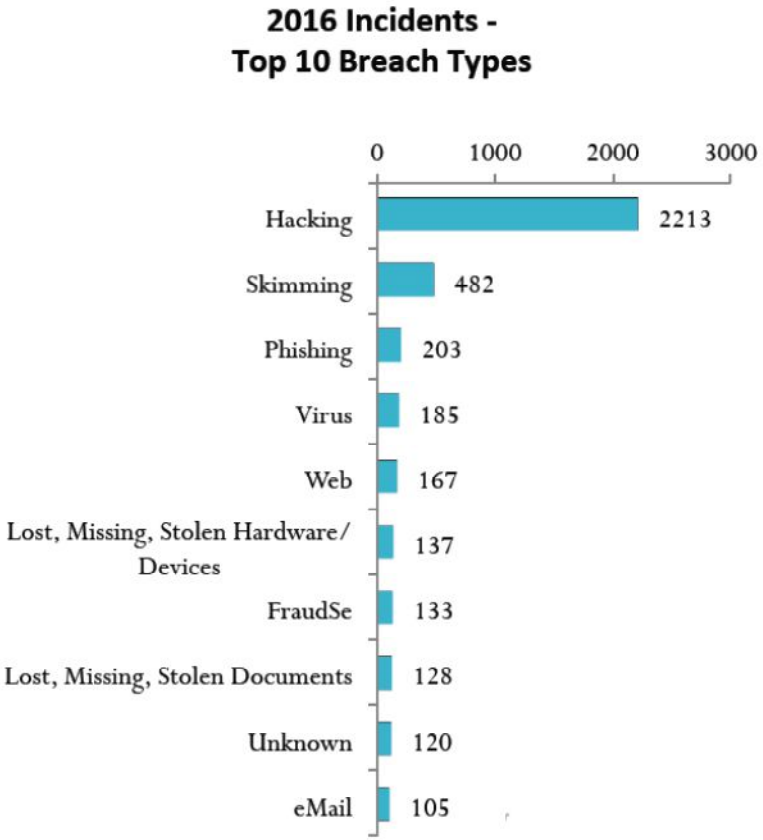
Source: Risk Based Security, 2016 Year End Data Breach Quick View Report.

2016 Cost of a Data Breach?

- Average Consolidated Cost: $4.0 Million
- Cost Per Breached Record: $158

Source: Ponemon Institute, 2016 Cost of a Data Breach Study.

What are the Sources of Data Breaches



Hacking continues to dominate as the leading breach type, with SQL injection a predominant method utilized.

Stolen laptops, once a leading cause of data compromise, accounted for only 67 (1.6%) of incidents in 2016.

Source: Risk Based Security, 2016 Year End Data Breach Quick View Report.

Who is Behind the Breach?

- State Actors
  - China
  - Iran
  - North Korea
  - Russia
- Organized Fraud Gangs for Profit
  - Eastern Europe/Russia
  - Nigeria
  - ISIS/Terrorist-Based Organizations
- Individual Free-Lance Hackers for Profit (Guccifer)
- Loosely Organized Ideology-Based Teams (Anonymous/Hacktivists)
- Miscellaneous Anarchists

Data Breach Scenario: Multinational Life Sciences Company

- Life Sciences Company:
  - Subsidiaries in Europe, South America and Asia
- Computer Servers and Individual Laptops Connected to Servers
  - PII of Employees: SSN, Payroll, Bank Account
  - PII of Patients Involved in Studies
  - Vendor/Partner/Customer Financial Information (Bank Accounts, Financials, FCPA Due Diligence)
  - Health Records of Patients Involved In Studies
  - Confidential Market/Strategy Information and Documents
  - Intellectual Property

Data Breach Scenario: The Virus

- Phishing Incident
  - Employee E-Mail in Europe
  - Infection Spreads to US
- Wannacry/EternalBlue Type Virus
  - Computer Uploads DoublePulsar Type Virus
  - Hackers Gain Administrator Status
  - Individual Computers Frozen with Ransom Demand
  - Hackers Start to Mine information from Servers/Computers
  - Files Transferred to Hackers

Incident Response Priorities

1. Containment

2. Triage
- What data? Where? Preservation?

3. Internal notifications
- Management / Board / Stakeholders

4. Involving outside experts
- Forensic experts, outside counsel, PR

5. Involving law enforcement?

6. External notifications
- By law (e.g., data subject / public / regulator notice per data breach notification laws)
- By contract (e.g., partners / third parties / vendors)

7. Other communications
- What to say to employees, vendors, and third parties?

8. Internal investigation (forensic; interviews)
- Scope of breach (How long? What types of data? How much?)
- Data protected (encrypted)? Extent of harm?
- Cause of breach? Attack vector?

9. Remediation

10. Preparation for government inquiries and litigation

Pre-Incident Preparedness Checklist

- ✓ Develop information governance controls
- ✓ Identify, map, and assess compliance with legal and regulatory obligations at federal, state, and international levels
- ✓ Establish legal work plan for cybersecurity crisis prevention and crisis management
- ✓ Develop and maintain written policy and procedures
- ✓ Develop and maintain training programs for employees and contractors
- ✓ Deploy appropriate information security safeguards for vendors/service providers, including reporting and due diligence
- ✓ Identify consulting and other outside resources
- ✓ Implement secure technology design
- ✓ Test and update all assessments, safeguards and protocols
- ✓ Maintain confidentiality