PORZIO BROMBERG&NEWMAN P.C.

PORZIO LifeSciences

SETON HALL | LAW

Cybersecurity 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

Fernando M. Pinguelo, JD, CIPP
Partner, Scarinci Hollenbeck; Chair of the firm's Cyber Security & Data Protection and E-Discovery groups, New York and Red Bank, NJ

David W. Opderbeck, PhD, JD, LLM
Seton Hall Law School Professor of Law and Co-Director of the Gibbons Institute of Law, Science & Technology.

William J. Hughes, Jr., JD, LLM
Principal, Porzio, Bromberg & Newman, P.C.; Assistant US Attorney and Trial Attorney, US Department of Justice, Morristown, NJ (Moderator)

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

The New York Times

MAY 12, 2017

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

2017 Data Breaches

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

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 and 2017

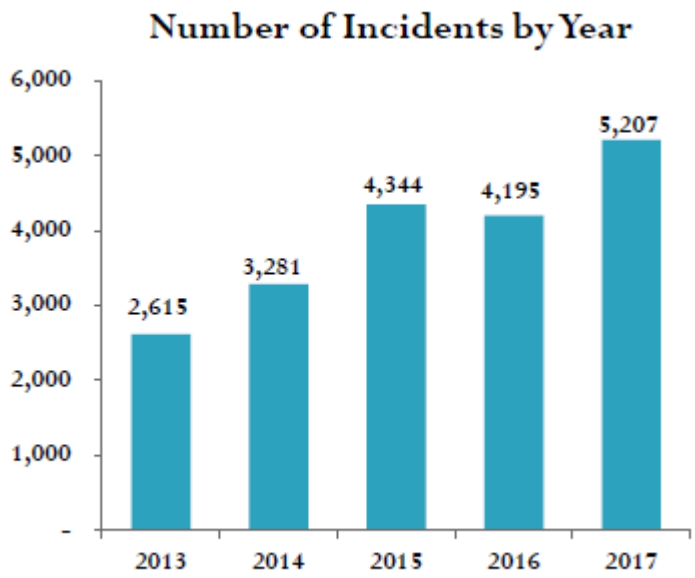
	2016	2017	Change
Reported Data Breaches:	4,195	5,207	+24.1%
Number of Records:	6.36 Billion	7.89 Billion	+24.3%

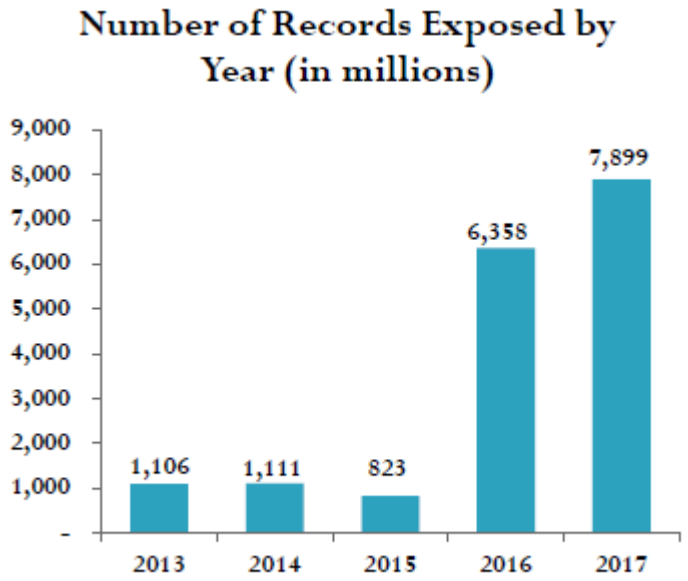
2017 Breakdown:

Threat Vector	Records Exposed
Inside-Accidental	3,079,361,872
Outside	2,738,517,484
Inside-Unknown	2,020,878,036
Unknown	59,590,961
Inside-Malicious	1,646,259
Total	**7,899,994,612**

Source: Risk Based Security, 2016 & 2017 Year End Data Breach Quick View Reports

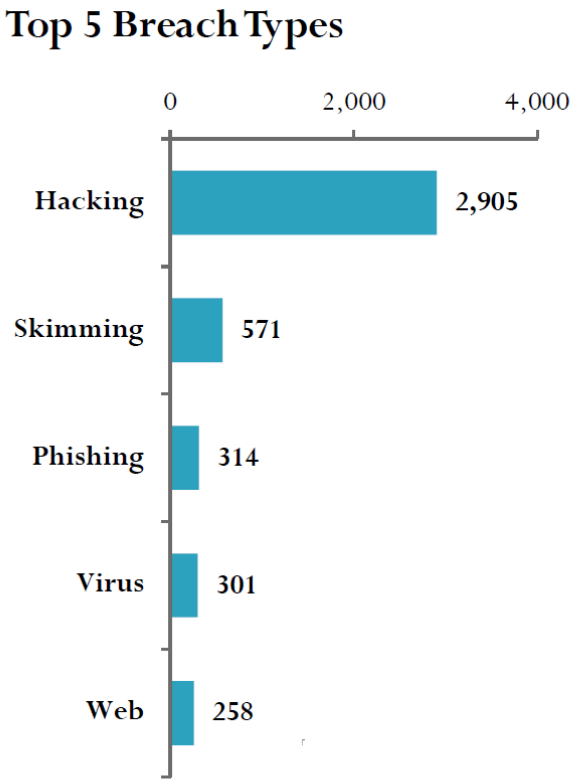
Historical Data Breaches by the Numbers





Source: Risk Based Security, 2017 Year End Data Breach Quick View Report.

What are the Sources of Data Breaches?



Hacking (unauthorized intrusion into systems or networks) is continuously the leading source of data breaches. However, 2017 saw the lowest percentage of records exposed by hackers since 2008, when 45.5% of exposed records were the result of hacking.

Source: Risk Based Security, 2017 Year End Data Breach Quick View Report.

2017 Cost of a Data Breach?

- **Data breaches are most expensive in the United States and Canada and least expensive in Brazil and India.**
- The average per capita cost of data breach was **$225 in the United States** and $190 in Canada. The lowest cost was Brazil ($79) and India ($64).
- The average total organizational cost **in the United States was $7.35 million** and $4.94 million in the Middle East. The lowest average total organizational cost was in Brazil ($1.52 million) and India ($1.68 million).

Source: Ponemon Institute, 2017 Cost of a Data Breach Study.

2017 Cost of a Data Breach

- **Certain industries have more costly data breaches.** The average global cost of data breach per lost or stolen record was **$141.** However, **health care organizations had an average cost of $380** and in financial services the average cost was $245. Media ($119), research ($101) and public sector ($71) had the lowest average cost per lost or stolen record.

Source: Ponemon Institute, 2017 Cost of a Data Breach Study.

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

Tabletop Exercises

- What is it?
- Why do it?
- How is it done?
- Who participates?
- How often?

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

Data Breach Scenario

- **Corporate IT Response**: Assessment, Containment and Recovery
- **Corporate Governance Response**: Assessment, Resource Allocation and Notification
- **Corporate Legal Response**: Assessment, Protection and Notification
  - Who to Notify?
  - Public Relations?
  - Fallout?
  - What happens after containment?

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


DON'T
PANIC!