



# Recent Attacks on Data Security: The Stuff of Nightmares!

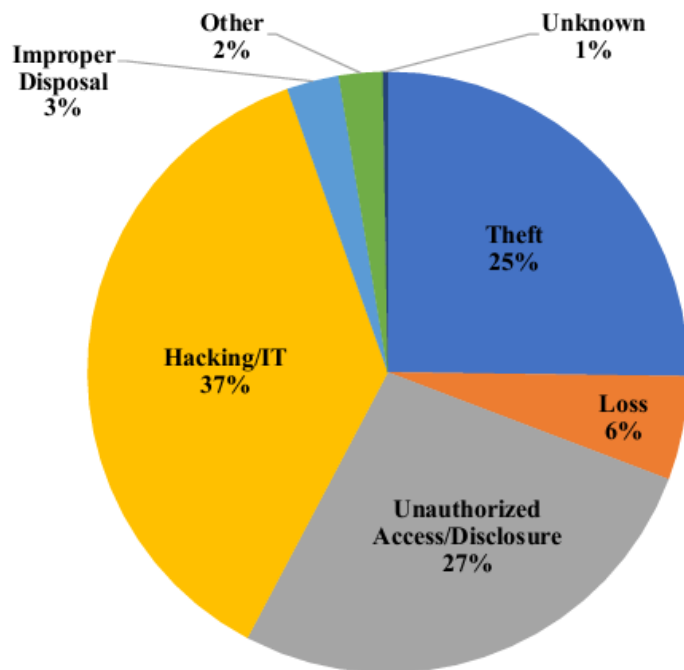
*Iliana L. Peters, J.D., LL.M., CISSP*

*John Bates, Senior Counsel at DocuSign*

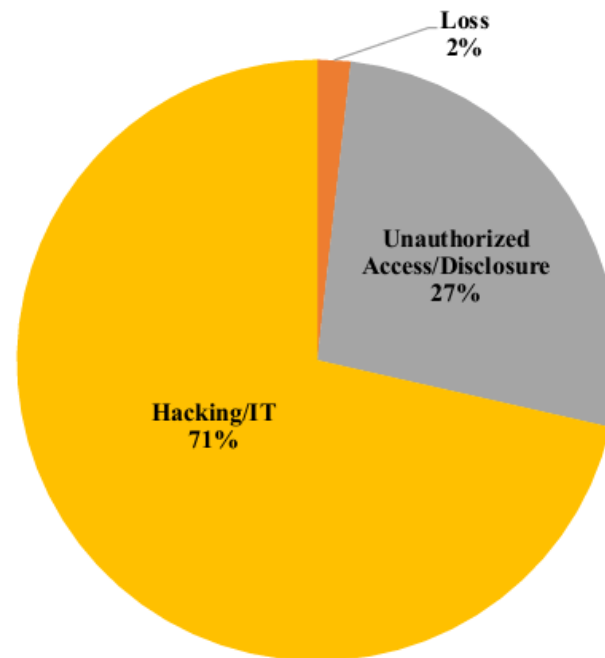
*April 20, 2021*

# HHS Breach Report

## 500+ Breaches by Type of Breach



September 23, 2009 through February 28, 2021



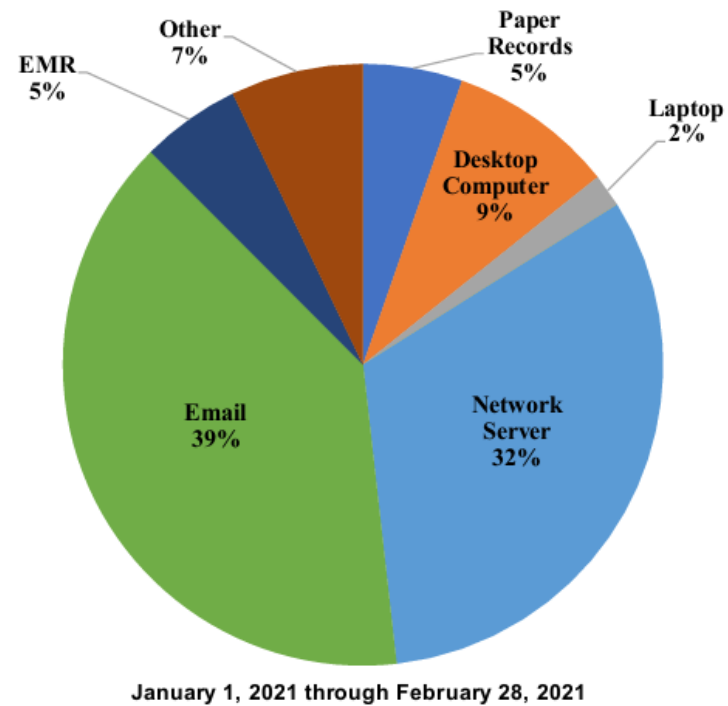
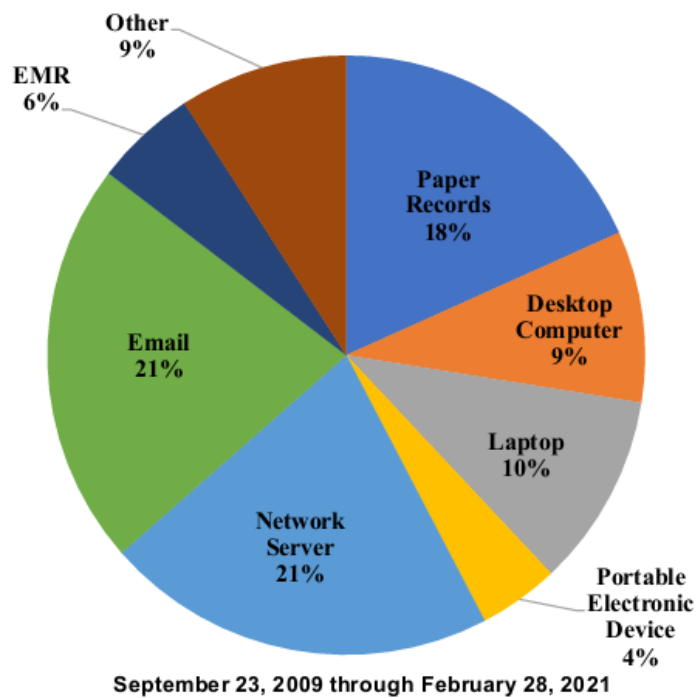
January 1, 2021 through February 28, 2021

# Threat Landscape

- Vast majority of Data has been created in the past couple of years.
  - Estimated 18 ZB (ZB:1M PB:1000 TB) in 2018 / 175 ZB in 2025 (DVDs circle earth 222 times).
- Cloud Engineering is very immature.
  - Cloud is being implemented without IT, Security, or Legal review/approval.
  - Business clients are highly sophisticated and can easily spin up Cloud services.
- Traditional IT Infrastructure resources can be resistant to learning new technology (Cloud)
  - Increasing Use of Third Party and Nth Party Vendors
  - Most US companies have experienced a data breach caused by Nth party.
  - Most companies do not have a comprehensive list of third-party vendors.
  - Nth parties are mostly unknown by most companies.
- NotPetya was a new type of attack in terms of damage and dollar amount.
  - Business Continuity cost Merck at least \$1.3B.
  - Maersk had to shift entire worldwide operations to paper. \$300M loss.
  - Modelez lost manufacturing and suffered \$700M loss.

# HHS Breach Report

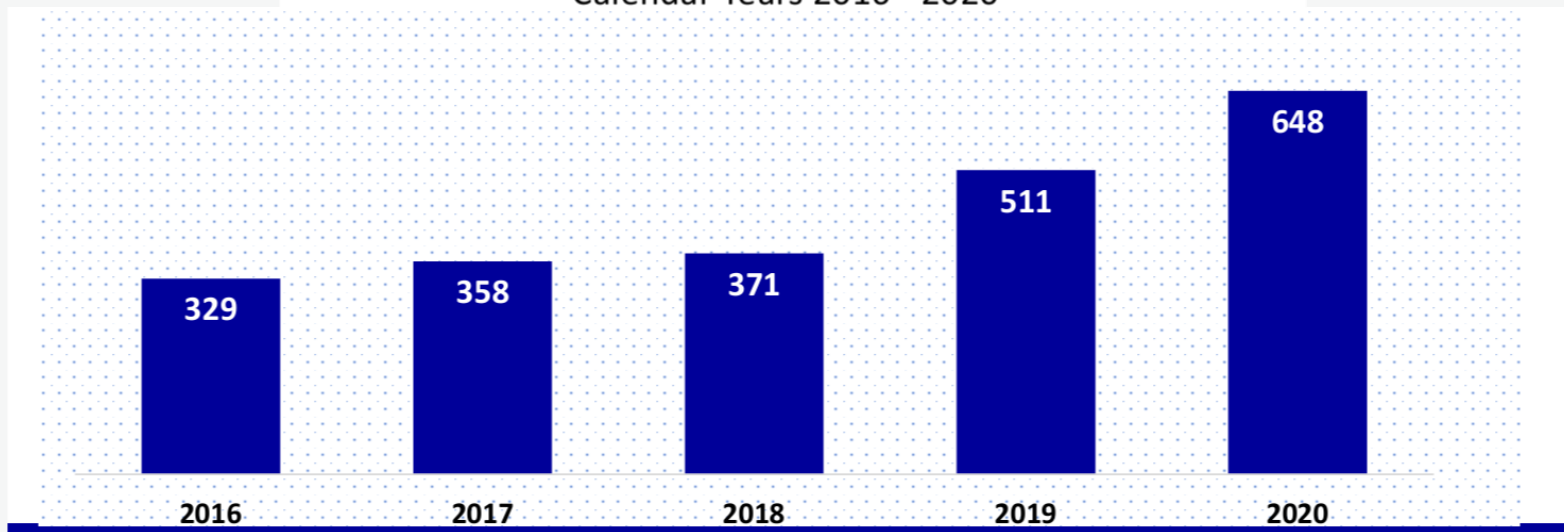
## 500+ Breaches by Location of Breach



# HHS Breach Report

## Breaches Affecting 500 or More Individuals Reports Received by Year

Calendar Years 2016 - 2020



# Know Your Regulator

- Department of Health and Human Services
  - Office for Civil Rights
  - Office of Inspector General
- Federal Trade Commission
- Federal Communications Commission
- Department of Justice
- State Attorneys General
- Other State Agencies
  - New York State Department of Financial Services (“NYDFS”)

# Regulator Activity

- Increasing Fines and Prescriptive Oversight.
  - FTC Facebook \$5B; Equifax \$575M; Lifelock \$100M; Uber \$148M with State AGs
  - OCR Sentara \$2.175M for 557 records; TX Health Services Commission \$1.6M for 6617 records; University of Rochester Medical Center \$3M for 43 records; Jackson Health System \$2.15M for 1500 records.
  - GPDR British Airways £183M; Marriott £100M; £60k fine for credentials that shared 1 record.

# Did you know?

- Current Data from 2020 ACC Foundation State of Cybersecurity Report
  - 33.6% of legal departments did not know how many breaches occurred in the past year.
  - 14.2% do not have an incident response plan / 9.9% don't know.
  - 19.3% do not have an IRT / 6.2% don't know.
  - 38.1% hold a simulated response exercise
  - 31.9% conduct tabletop exercises.
  - 6.9% conduct quarterly cybersecurity audits.



# Cyber Attack Response Considerations

- Identify appropriate point(s) of contact
- “Stop the Bleeding” (Identify, Triage, Contain, Eradicate)
- Preserve Evidence
- Contact Cyber Insurer
- Engage Outside Counsel
- Engage Forensic Vendor through Counsel
- Determine Scope
- Coordinate with ISOs/ISAOs
- Coordinate with Law Enforcement
- Analyze Notification Responsibilities
- Engage Notification Vendor
- Prepare for Regulatory Investigations

# Technical and Legal Considerations

- Business Associate Agreements
- Lack of Inventory of Data & Assets
- Risk Analysis
- Detect or Manage Identified Risk
- End-to-end Encryption
- Transmission Security; Lack of Security: Data at Rest & Archived Data
- Appropriate Auditing
- Patch management of Software, Systems, Firmware, Devices
- Vulnerability scanning
- Penetration testing
- Security awareness program for end users (e.g., phishing and other threats)
- Insider Threat (negligent & malicious)
- Disaster recovery and business continuity plans & teams
- Incident response plans & teams

- DOJ Guidelines on Evaluating Compliance Programs (included detailed checklist)
  - Risk Assessment
  - Policies & Procedures
  - Training & Communications
  - Confidential Reporting Structure & Investigation Process
  - Third-Party Management
- Speaking Security Lingo is important to creating rapport.
  - List from ACC Cybersecurity Summit


# Conclusions and Recommendations

- **Do you have a handle on all of your data?**
  - PII? PHI? IP? Other sensitive or proprietary data?
- **What laws apply to your data?**
  - State? Federal? International?
- **Consider all potential risks!**
  - State, Federal, International civil and criminal actions;
  - Litigation, including class actions.
- **Coordinate closely with counsel.**

# Questions?

- Iliana L. Peters

[IPeters@Polsinelli.com](mailto:IPeters@Polsinelli.com)



Polsinelli PC provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should 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.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

© 2020 Polsinelli® is a registered trademark of Polsinelli PC. Polsinelli LLP in California. Polsinelli PC (Inc.) in Florida.

[polsinelli.com](https://www.polsinelli.com)

