

# DATA PRIVACY INCIDENTS:

---

What Every In-House Counsel Needs to  
Know

BakerHostetler



# Presenters:



**Danielle Wesley, Esq.**  
Vice President and General Counsel  
MRO Corp.  
T + 1.610.994.7500 Ext. 583  
[dwesley@mrocorp.com](mailto:dwesley@mrocorp.com)

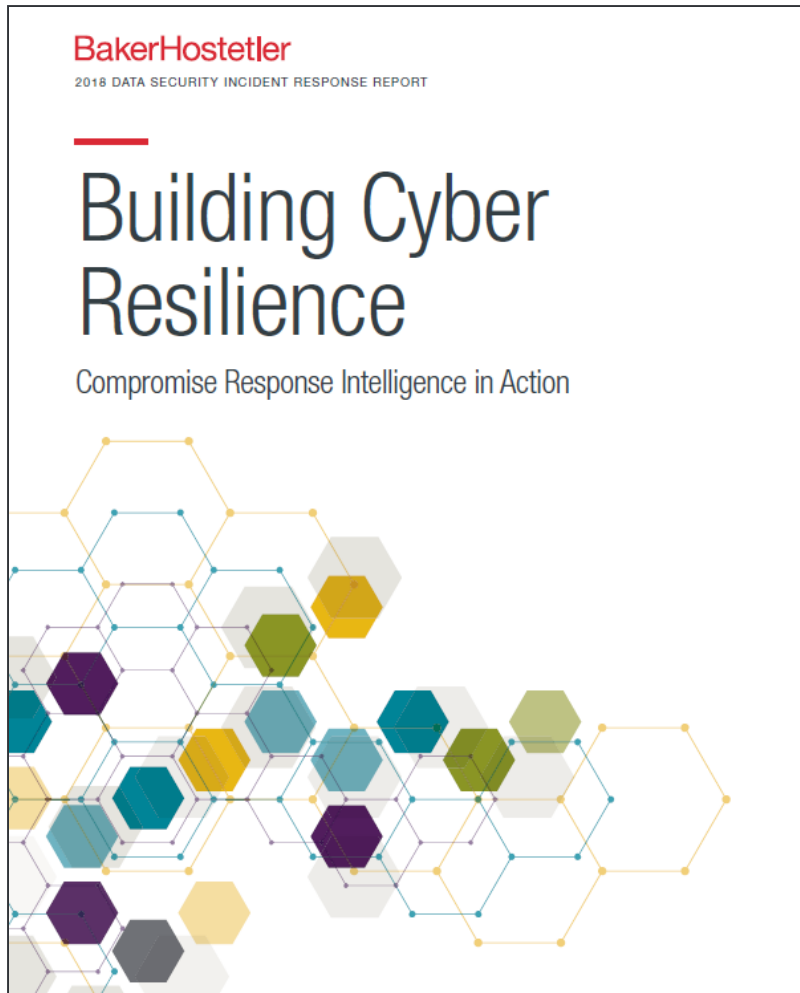


**Eric A. Packel**, Partner  
BakerHostetler  
Philadelphia  
[epackel@bakerlaw.com](mailto:epackel@bakerlaw.com)  
T +1.215.564.3031



**Sara M. Goldstein**, Associate  
BakerHostetler  
Philadelphia  
[sgoldstein@bakerlaw.com](mailto:sgoldstein@bakerlaw.com)  
T +1 215.564.1572

# Introduction



## BakerHostetler

- Chambers USA 2018 nationally ranked & Legal 500 ranked Privacy and Data Protection practice
- Privacy and Data Protection “Practice Group of the Year” by Law360 in 2013, 2014, 2015, and 2018
- More than 3,500 incidents handled (750+ in 2018 alone)
- Team includes 60+ attorneys specializing in privacy and data security law across the country

# Program Overview



# Cyber Risks

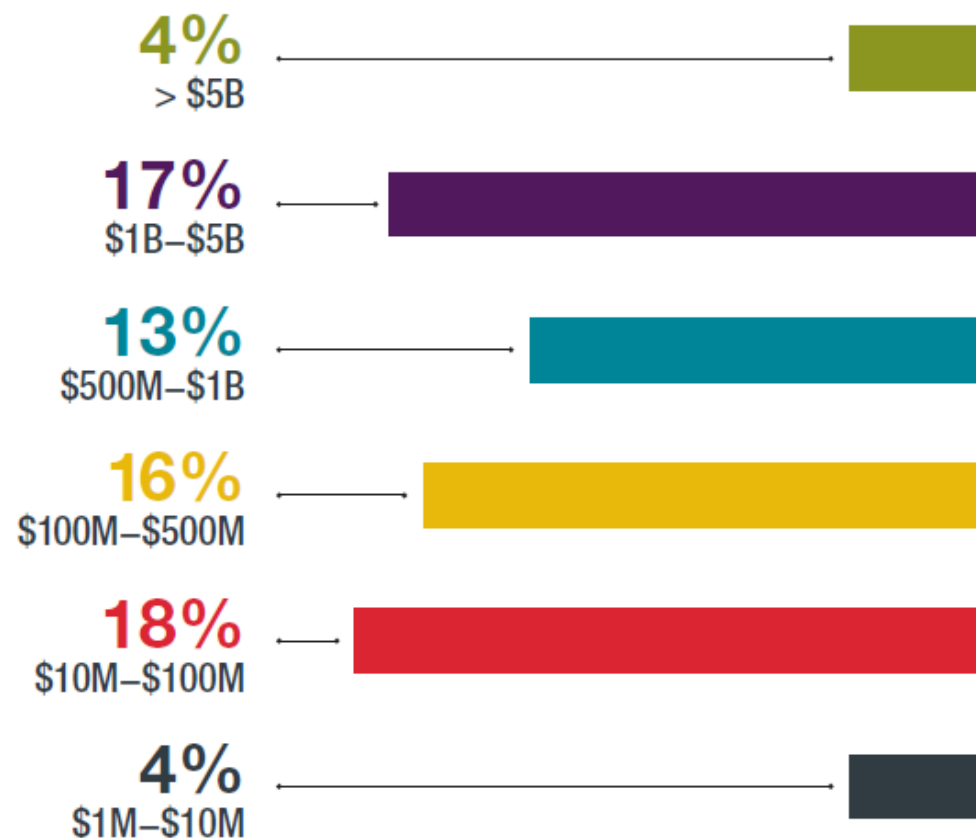


"A Frightening New Kind of DDoS Attack is Breaking Records" – *Forbes*, March 7, 2018.

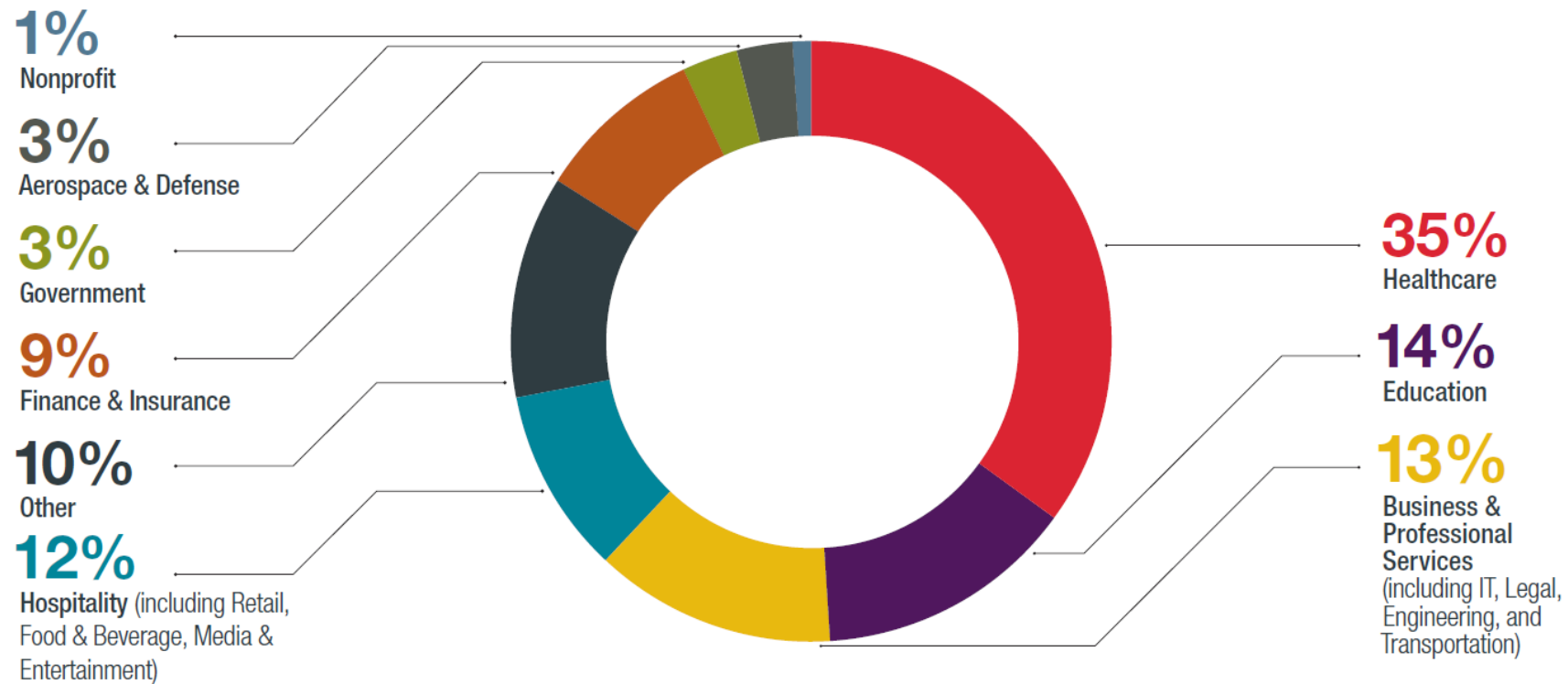
Phishing Attacks Targeting W-2 Data Hit 41 Organizations in Q1 2016 – *CSO* from IDG.

Sony Hackers Used Phishing Emails to Breach Company Networks – *Krebs on Security*.

Entity Size by Revenue



# Industries Affected




# Incident Causes



**34%**  
Phishing

**32%**  
Involved Remote  
Access


**18%**  
Involved  
Ransomware



**19%**  
Network Intrusion

**38%**  
Involved Ransomware


**17%**  
Involved Automated  
Data Exfiltration



**17%**  
Inadvertent Disclosure



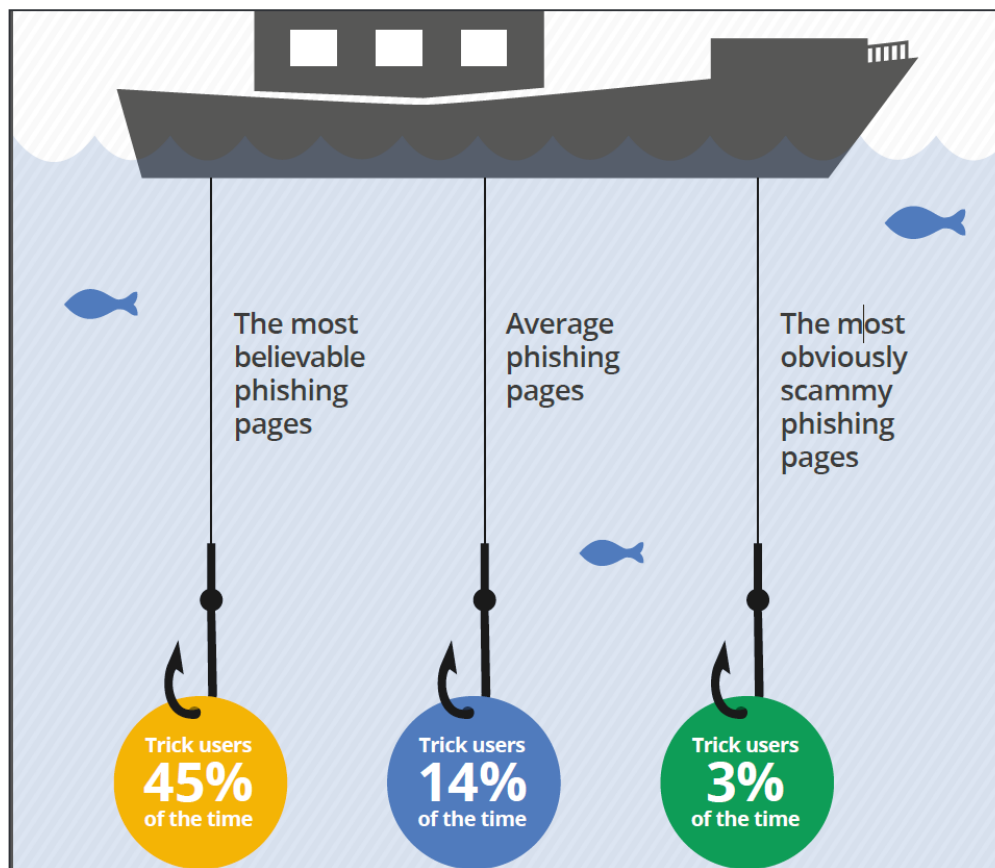
**11%**  
Stolen/Lost Device  
or Records



**6%**  
System Misconfiguration

# Phishing Schemes

Cyber Extortion #Trending

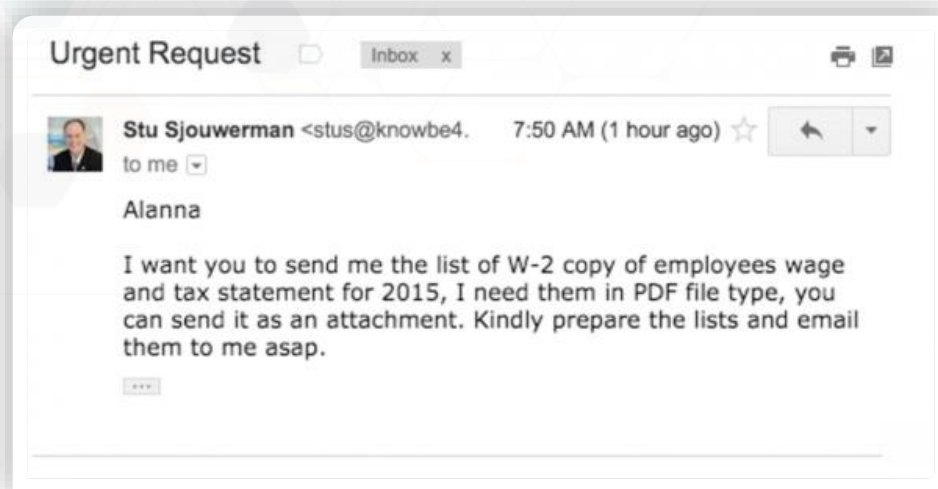


- **Phishing Schemes**
  - W2 / Tax Related
  - Requests for wires
  - Payroll ACH Fraud
- 20% of hackers access compromised accounts within 30 minutes of getting their credentials
- Hackers spend on average 3 minutes searching the account for valuable information, such as “wire transfer” and “bank”
- Compromised accounts are used to send SPAM or phishing attacks using your address book



## Common Phishing Technique:

- 🚩 Hackers use emails from a target organization's CEO, asking human resources and accounting departments for employee W-2 information:



## New Area Prone to Attack:

- 🚩 In 2017, hackers phished online payroll management account credentials used by corporate HR professionals.



# PHISHING



## Best Practices:

- ✓ Train employees to spot phishing emails. Utilize test-phishing campaigns as a training device.
- ✓ Educate employees not to provide login credentials or use the same credentials for multiple sites.
- ✓ Enable Multi-Factor Authentication (MFA) throughout your entity.

# Ransomware

## WannaCry Attack – Threat or Fake News?:

- ✖ A ransomware attack that impacted more than 300,000 people across 150 countries in less than two days.

✖ - Stroz Friedberg, *2018 Cybersecurity Predictions*, at p. 18 (2018)

## How it Happens:

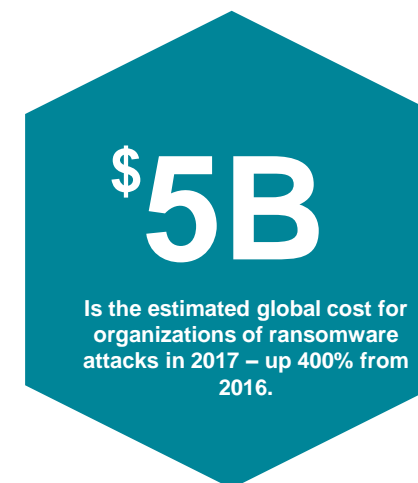
- ✖ Hackers gain access to your computer's file system by installing a program via phishing link/attachment or by poorly configured Remote Desktop Protocol service.
- ✖ The ransomware prevents a user from accessing the operating system, or encrypts all the data stored on the computer.
- ✖ The hacker asks the user to pay a fixed amount of money (the ransom) to decrypt the files or allow access to the operating system.

## Best Practices:

- ✓ Maintain a robust, off-site backup of data
- ✓ Properly configure Remote Desktop Protocol services.

*Criminals will evolve their tactics, including launching well-researched, targeted attacks intended to infect specific high-value assets known to hold critical data.*

✖ Stroz Friedberg (AON), *2018 Cybersecurity Predictions*, at p. 18 (2018).



# Ransomware on the Rise



**70%**

Of businesses paid the  
ransom to get their data  
back in 2016

**\$8,500**

Lost per hour due to downtime  
caused by ransomware

## RANSOMWARE

### AVERAGE PAYMENT

**\$40,000**



**100% relied on  
vendor when  
payment in bitcoins  
was requested.**

## Incident Response Timeline



# 66

Days

Occurrence to Discovery



# 3

Days

Discovery to Containment



# 36

Days

Time to Complete Forensic Investigation



# 38

Days

Discovery to Notification

OCCURRENCE

DISCOVERY

NOTIFICATION



CONTAINMENT

FORENSIC INVESTIGATION COMPLETE

Occurrence

Discovery

Containment

Forensic Investigation

Notification



# The Privacy “Patchwork”

- Federal & state laws govern the handling of PII/PHI
  - Laws covering SSNs / disposal of PII
  - Employment-related laws (e.g., FMLA, ADA, GINA)
  - Other federal and state regulations (e.g., FTC Act, Mass. Regs)
- HIPAA
  - Applies to Covered Entities and Business Associates
  - Preempted except where state law is “more stringent”
- State breach notification laws
- State medical information breach reporting laws
- International data protection regulations





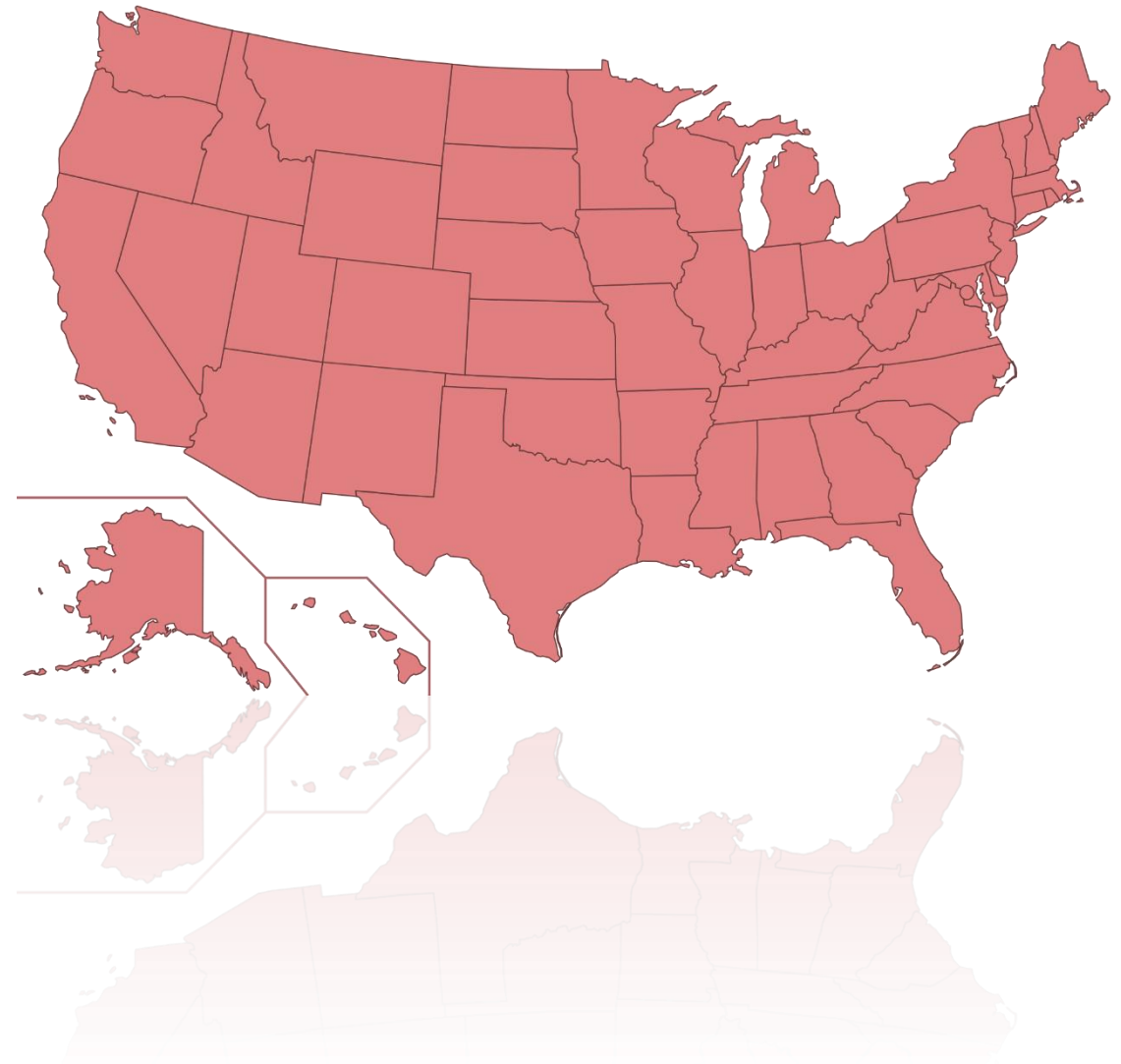
# Federal Trade Commission (FTC)

- Section 5 Broad Enforcement Authority
  - Concerns “unfair” and “deceptive” trade practices
  - FTC: de facto privacy law regulator in the U.S.
- Regulates privacy/data security in the absence of statutory authority through enforcement actions and consent orders
  - Failure to adequately disclose data collection/sharing practices
  - Broken privacy/data security practices
  - Failure to take reasonable steps to maintain security of data-strict liability
- Over 40 General Privacy Cases to Date



# State Laws

- 50 States, D.C., & U.S. territories
- Laws vary between jurisdictions
- Varying levels of enforcement by state attorneys general
- Limited precedent
  - What does “access” mean?
  - What is a reasonable notice time?



# California Consumer Privacy Act (CCPA) Snapshot

- Effective January 1, 2020
- Regulates both privacy and data security
- Privacy
  - Consumers have certain rights regarding their Personal Information (“PI”)
    - Rights of information, access, portability, and deletion
    - Right to prohibit the sale of their PI
      - Opt-out rights, except opt-in for under 16
    - Businesses may not “discriminate” for exercise of rights
- Security
  - Businesses must implement “reasonable” data security
    - No significant change from current CA data breach and security requirements, except...
  - Private right of action created for individuals affected by certain types of data security incidents

# Who does GDPR apply to? Can it apply to US companies?

- GDPR applies to organizations that:
  1. Are “established” in the EU or EEA;
  2. Process personal data of EU “data subjects” when offering them goods or services (whether or not for payment); or
  3. Monitor behavior occurring in the EU

***It can DEFINITELY apply to US companies!***





- ❖ Digital Privacy Act (amending Canada's foundational Personal Information Protection and Electronic Documents Act (PIPEDA)) became law on June 18, 2015:
  - ❖ Includes federal security breach notification requirement
  - ❖ Implementing regulations were issued by the Canadian Government and went into effect on November 1, 2018.
- ❖ Requirement to report to the Privacy Commissioner and any affected individuals "any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual"
- ❖ Definition of "significant harm" is broad (includes, e.g., humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities)
- ❖ Factors to consider when assessing the risk of "significant harm" include the sensitivity of the PI and the probability of misuse
- ❖ Details concerning the form, manner, and content of the required notifications, as well as additional factors relevant to the risk assessment, are to be spelled out in the forthcoming regulations
- ❖ Digital Privacy Act provides for fines of up to CA\$100,000 for knowing violations of the breach notification requirements
- ❖ Previously, Alberta was the only province with a mandatory private sector-wide breach notification requirement:
  - ❖ Others have specific notification requirements (health data breaches) and/or have proposed notification requirements that likely will be superseded by the federal law



## Australia

- Notification required if a “reasonable person” would conclude the incident would be likely to result in serious harm to any individuals whose information was affected.

## Japan

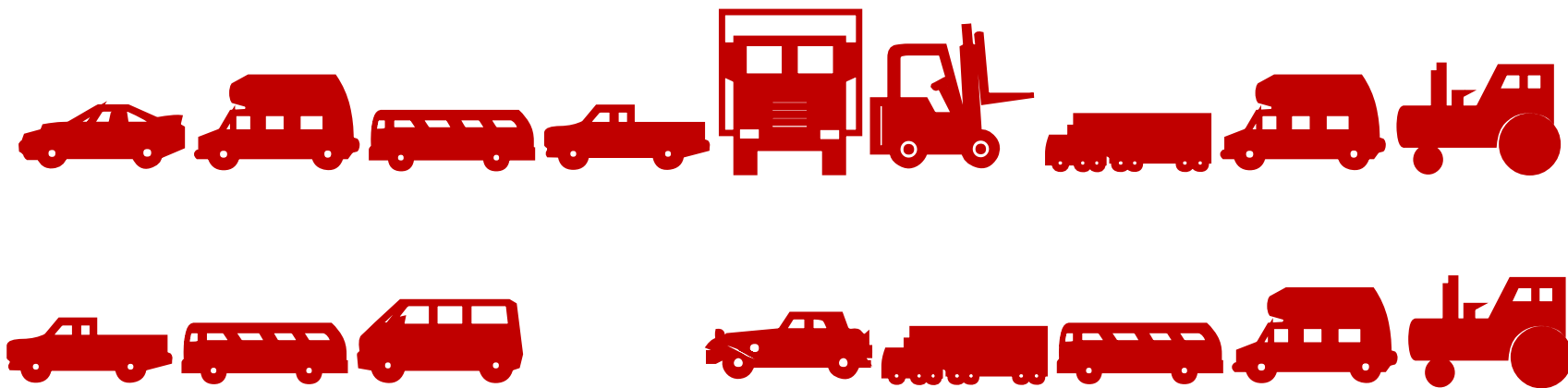
- Guidelines advise notifying affected data subjects and possibly the Commissioner of leakage, destruction or damage of personal information; also advise public announcement

## Bermuda

- Requires notification to the DPA and affected individuals for security breaches that lead to the loss or unlawful destruction or unauthorized disclosure of, or access to, personal information that is likely to adversely affect an individual.

## Singapore (Proposal)

- Currently has a voluntary notification regime; on July 27, 2017 authorities proposed mandatory notification to the commission and affected individuals.
- Requirement would apply to:
  - Breaches that pose “any risk of impact or harm to the affected individuals “
  - Breaches of significant scale (500+ affected), even if there is no risk of harm.

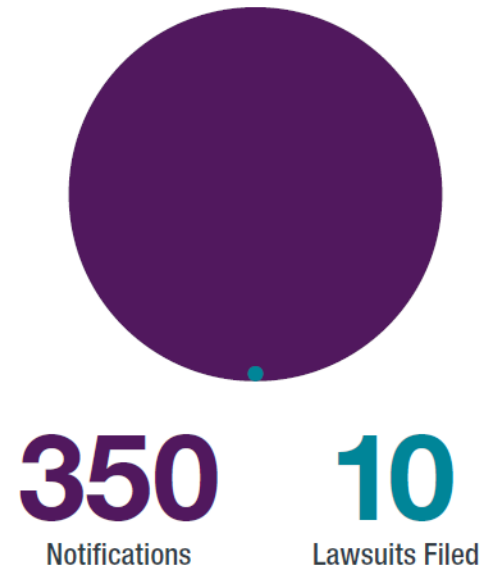




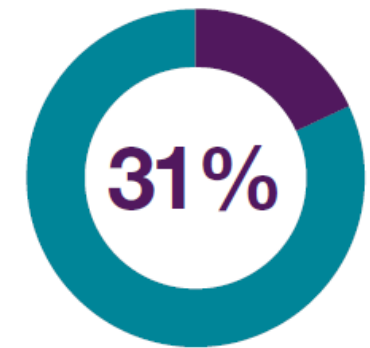
# After You've Mailed Notice...

- Business may suffer reputational harm.
- Business may receive AG, DOI or other regulatory inquiries, investigations or litigations, as well as consumer or contractual lawsuits.
- Impact in business operations and a disruption in productivity may result.

Notifications vs. Lawsuits Filed



AG Inquiries Following Notification



Non-AG Inquiries



# Enforcement Actions by Attorneys General

- Settlement Reached Between Neiman Marcus and State Attorneys General for \$1.5 Million for 2013 Payment Card Breach (January 7, 2019)
- State Attorneys General Announce Record \$148 Million Settlement With Uber Over 2016 Data Breach (September 26, 2018)
- 47 states and D.C. reach a \$18.5 million settlement with the Target Corporation to resolve the states' investigation into the retail company's 2013 data breach (December 13, 2017)

# OCR Resolution Agreements

- Providence Health & Services (\$100K)
- CVS Pharmacy (\$2.25M)
- Rite-Aid (\$1M)
- Management Services Organization of Washington (\$35K)
- Cignet (\$4.3M)
- Massachusetts General Hospital (\$1M)
- UCLA Health Services (\$865K)
- Blue Cross Blue Shield of Tennessee (\$1.5M)
- Alaska Medicaid (\$1.7M)
- Phoenix Cardiac Surgery, P.C. (\$100K)
- Massachusetts Eye and Ear Infirmary (\$1.5M)
- Hospice of North Idaho (\$50K)
- Idaho State University (\$400K)
- Shasta Regional Medical Center (\$275K)
- WellPoint (\$1.7M)
- Affinity Health Plan (\$1.2M)
- Adult & Pediatric Dermatology, P.C. of Massachusetts (\$150K)
- Skagit County, Washington (\$215K)
- QCA Health Plan, Inc. (\$250K)
- Concentra Health Services (\$1.725M)
- New York and Presbyterian Hospital (\$3.3M)
- Columbia University (\$1.5M)
- Parkview Health System (\$800K)
- Anchorage Community Mental Health Services (\$150K)
- Cornell Prescription Pharmacy (\$125K)
- St. Elizabeth's Medical Center (\$216.4K)
- Cancer Care Center (\$750K)
- Lahey Hospital and Medical Center (\$850K)
- Triple-S Management Corporation (\$3.5M)
- University of Washington Medicine (\$750K)
- Lincare (\$239.8K)
- Complete P.T. Pool & Land Physical Therapy (\$25K)
- North Memorial Healthcare (\$1.55M)
- Feinstein Institute for Medical Research (\$3.9M)
- Raleigh Orthopaedic Clinic, PA of N. Carolina (\$750k)
- New York Presbyterian Hospital (\$2.2M)
- Catholic Health Care Services of the Archdiocese of Philadelphia (\$650K)
- Oregon Health & Science University (\$2.7M)
- University of Mississippi Medical Center (\$2.75M)
- Advocate Health Care Network (\$5.55M)
- Care New England Health System (\$400K)
- St. Joseph Health (\$2.14M)
- University of Massachusetts Amherst (\$650K)
- Presence Health (\$475K)
- Children's Medical Center of Dallas (\$3.2M)
- Memorial Healthcare System (\$5.5M)
- Metro Community Provider Network (\$400K)
- The Center for Children's Digestive Health (\$31K)
- CardioNet (\$2.5M)
- Memorial Hermann Health System (\$2.4M)
- St. Luke's-Roosevelt Hospital Center (387K)
- 21<sup>st</sup> Century Oncology (\$2.3M)
- Fresenius Medical Care North America (\$3.5M)
- Filefax (\$100K)
- The University of Texas MD Anderson Cancer Center (\$4.5M)
- Boston Medical Center (\$100K)
- Brigham & Women's Hospital (\$384K)
- Massachusetts General Hospital (\$515K)
- Anthem, Inc. (\$ 16M)
- Allergy Associates of Hartford, P.C. (\$125K)
- Advanced Care Hospitalists PL (\$500k)
- Pagosa Springs Medical Center (\$111k)
- Cottage Health (\$3M)

# The FTC Act Enforcement Actions

- PaymentsMD
  - The FTC settled allegations that a medical billing company collected consumers' personal medical information without their consent.
- GMR Transcription Services
  - Settlement involved allegations that a medical transcription company outsourced services to a third party without adequately checking to make sure it could implement reasonable security measures.
- Accretive Health
  - Company providing medical billing and revenue management services to hospitals put consumers' personal information at risk by (among other things) transporting laptops with sensitive data in a way that made them vulnerable to theft.
  - The FTC also said the company gave access to personal information to employees who didn't need it to do their jobs.

# Fines for Personal Data Breaches

- **Potential for Huge Sanctions:** Maximum fine for serious infringements of the GDPR is the greater of €20 million and 4% worldwide annual turnover
- Single GDPR fine issued for a personal data breach
  - German State supervisory authority imposed a €20,000 fine on a company for failing to hash passwords leading to a breach
- **Expect (significant) fines to be issued in 2019;** backlog of thousands of breach notifications
- Authorities may consider a **number of factors** when assessing fines, including (i) if the violation was intentional or negligence, (ii) if the company took action to mitigate the harm, (iii) if the company is a repeat offender, (iv) whether the company is cooperating with the Supervisory Authority, and (v) whether the company self-reported the violation.
- **Fines continue to be issued under pre-GDPR law;** fines are higher than in prior years



# Regulators Expect:

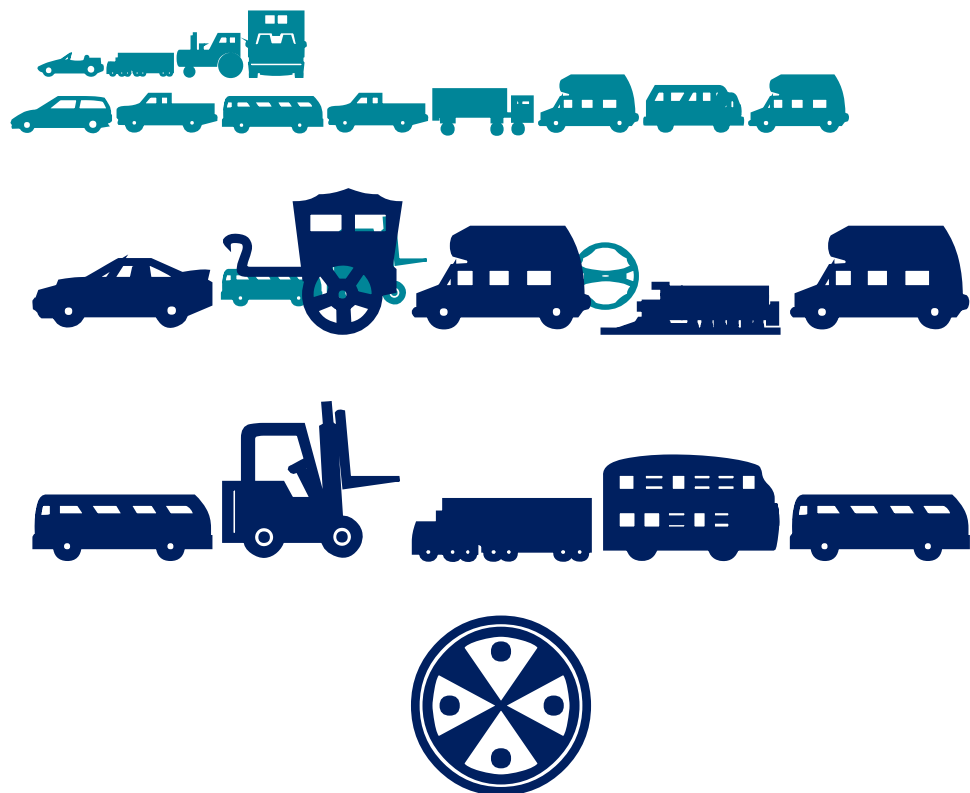
- ❖ Transparency: No Cover Ups.
- ❖ A prompt and thorough investigation.
- ❖ Good attitude and cooperation (commitment to compliance and safeguarding PII).
- ❖ Appropriate and prompt notification.
- ❖ Corrective action (know the root cause and address it; staff training; awareness program; technical safeguards; new policies/procedures/physical safeguards).
- ❖ Remediation and mitigation.



# Regulatory “Hot Buttons”



- Encryption of Portable Devices
- Two-Factor Authentication for Remote Access
- Patching
- Intrusion Detection Software
- Anti-Virus Software
- Logging / Access Controls
- Device Inventory, Tracking, and Monitoring
- Third Party Access to Data
- Security Awareness and Training
- Ignoring (or not completing) Risk Assessments
- Slow Detection
- Slow Notification
- Repeat Offenders





## BASIC DATA SECURITY BEST PRACTICES

- ❖ Data Identification & Classification
- ❖ Data hygiene don't collect what you don't need)
- ❖ Access restrictions
  - ❖ Is there a need for this employee to handle PII?
- ❖ Education
  - ❖ Does the workforce know how to identify and safeguard personal information?
  - ❖ Does workforce understand the importance of data security compliance
- ❖ Document retention/destruction

## PREVENTION = PROTECTION

- ❖ Vendor Management
- ❖ Security Awareness/Education
- ❖ Basic Data Security Good Practices
- ❖ Risk Assessment
- ❖ Policies and Procedures
- ❖ Consistent Enforcement of Policies and Procedures
- ❖ Practice breach response initiative
- ❖ Delete data when it is no longer needed

# Security Awareness & Education

## **Train employees at the time of hiring.**

- ❖ How do employee's spot security problems?
- ❖ What is the reporting procedure?
- ❖ Are leaders trained to handle reports from staff (e.g., is a gag order appropriate)?

## **Continue training employees regularly throughout their employment.**

- ❖ What does your training program include for security issues and procedures? Annual?
- ❖ Formal online training course vs. in-person?
- ❖ Monthly staff meetings?
- ❖ Newsletters?

# Risk Assessment

- ❖ Periodic Review of Administrative Safeguards
- ❖ Periodic Review of Physical Safeguards
- ❖ Periodic Review of Technical Safeguards
- ❖ Periodic Review of Data Flows – has the quantity/nature/sensitivity of the data changed?

# Policy & Procedures

- ✚ Security Incident Response Plan
- ✚ BYOD Policy and Social Media Policy
- ✚ Information Security and User Policies
  - ✚ What users can and must do to use network and organization's computer equipment.
  - ✚ Define limitations on users to keep the network secure (password policies, use of proprietary information, internet usage, system use, remote access)
- ✚ IT Policies
  - ✚ Virus incident and security incident
  - ✚ Logs
  - ✚ Backup policies
  - ✚ Server configuration, patch update, modification policies
  - ✚ Firewall policies
  - ✚ Wireless, VPN, router, and switch security
  - ✚ Email retention

## ✚ General Policies

- ✚ Program Policy
- ✚ Crisis Management Plan
- ✚ Disaster Recovery
  - ✚ Server Recovery
  - ✚ Data Recovery
  - ✚ End-user Recovery
  - ✚ Phone System Recovery
  - ✚ Emergency Response Plan
  - ✚ Workplace Recovery

# Questions



**Danielle Wesley, Esq.**

**Vice President and General Counsel  
MRO Corp.**

**T + 1.610.994.7500 Ext. 583**

**[dwesley@mrocorp.com](mailto:dwesley@mrocorp.com)**

**Eric A. Packel**

**Partner**

**Baker & Hostetler LLP**

**215.564.3031**

**[epackel@bakerlaw.com](mailto:epackel@bakerlaw.com)**

**Sara M. Goldstein**

**Associate**

**Baker & Hostetler LLP**

**215.564.1572**

**[sgoldstein@bakerlaw.com](mailto:sgoldstein@bakerlaw.com)**