



APRIL 13, 2022

# Data Privacy Trends & Cybersecurity Preparedness

Presented By | Colman McCarthy & Josh Hansen



SHOOK  
HARDY & BACON



## Colman McCarthy

*Partner* | Kansas City, Los Angeles

816.559.2081

[cdmccarthy@shb.com](mailto:cdmccarthy@shb.com)



## Josh Hansen

*Associate* | Denver

303.285.5306

[jahansen@shb.com](mailto:jahansen@shb.com)



- 01 Data Privacy Overview & Trends**
- 02 Legislative Update**
- 03 Cybersecurity Risks and Preparedness**
- 04 Q&A**



# Data Privacy Overview

# Privacy Law Concepts: Sources of Obligations

## State Comprehensive Laws

- Consumer Privacy – provides various protections described later

## State Breach Notification Laws

- Consumer Protection – requires notice if name + SSN, DL, etc. were improperly shared

## Federal Sectoral Laws

- Health Care Privacy (HIPAA) – safeguards electronic health information
- Financial Privacy (Gramm-Leach-Bliley Act) – affects non-public information held by financial institution

# Privacy Law Concepts: Terminology

Controller / Business	•Decides the purposes and means of processing (i.e., what to collect, why, how, for what purpose, and with whom to share it)
Processor / Service Provider	•Processes personal information (PI) on behalf of the controller/business; does not use PI for any other purpose, including a commercial one
Process/Processing	•Any action performed on PI, including collection, sale, storage, disclosure, analysis, deletion, modification
Sensitive Personal Information	•Racial/ethnic origin, religious beliefs, mental/physical health condition/diagnosis, sex life, sexual orientation, citizenship/citizenship status, genetic or biometric data for uniquely identifying an individual
Sale	•The exchange of PI for monetary or other valuable consideration
Profiling	•Automated processing to evaluate, analyze, or predict personal aspects related to economic situation, health, personal preferences, interests, reliability, behavior, location, or movements
Targeted Advertising	•Displaying advertisements to a consumer based on PI obtained from their activities over time and across nonaffiliated websites or online applications to predict preferences or interests

# State Laws: Rights & Obligations

## Consumer Rights

- Access (including data portability)
- Correction
- Deletion
- Opt-out of certain processing
- Opt-in to certain processing

## Controller Obligations

- Transparency
- Data Minimization
- Secondary Use Limitation
- Duty of Care
- Risk Assessment

## Processor Obligations

- Follow controller's instructions
- Assist with consumer requests
- Appropriate security, including of sub-processors
- Confidentiality
- Delete/return data
- Demonstrate compliance

## State Laws: Practical Considerations

- **Know your data**
  - Understand the content (What? Why?)
  - Create data maps (How? Where?)
- **Develop data subject request processes**
- **Understand your practices**
  - Draft accurate/digestible privacy notices
  - Ensure adequate safeguards
- **Update your contracts**



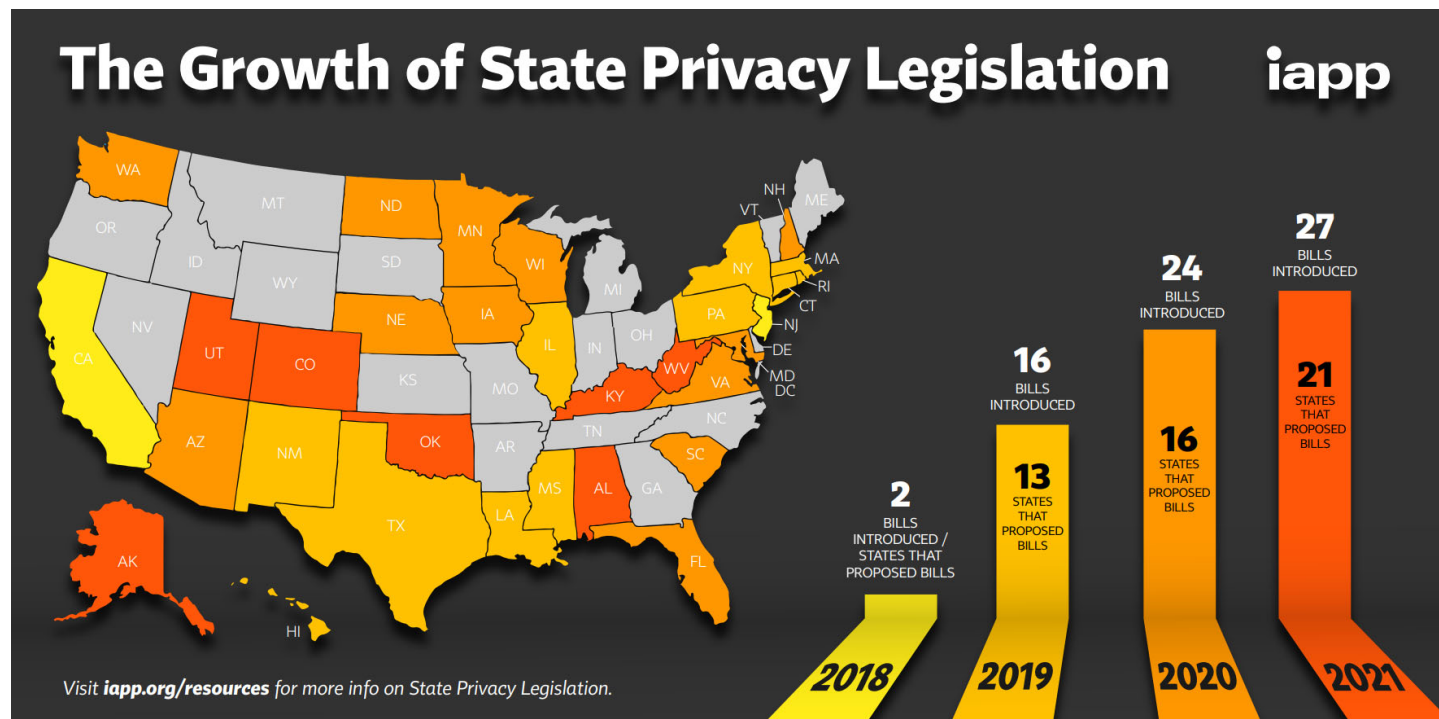


**POLL**



# Legislative Trends

# Pending Legislation



# Data Broker: Laws & Legislation



- Existing Laws
  - California (register)
  - Nevada (honor opt-outs)
  - Vermont (register & security measures)



- Legislation
  - Federal (register, audit, opt out)
  - Federal (register & security)
  - Alaska (register, 3% tax, and general privacy obligations)
  - Delaware (register & security measures)
  - Massachusetts (register, notice pre-sale, and general privacy obligations)



- Oregon (register)
- Washington (register, security, and general privacy obligations)



# Biometric Privacy: BIPA & Beyond

SHOOK, HARDY & BACON

## The Basics

- Written notice & consent before collecting biometric identifiers (fingerprint, voice scans, facial recognition, etc.)

## Illinois

- The focal point because private right of action
  - Active plaintiffs' bar – more than 1,450 suits [50+ this year]
  - Statutory damages (and large settlements)

## Washington/Texas

- AG enforcement with only 1 suit (TX v. Meta)

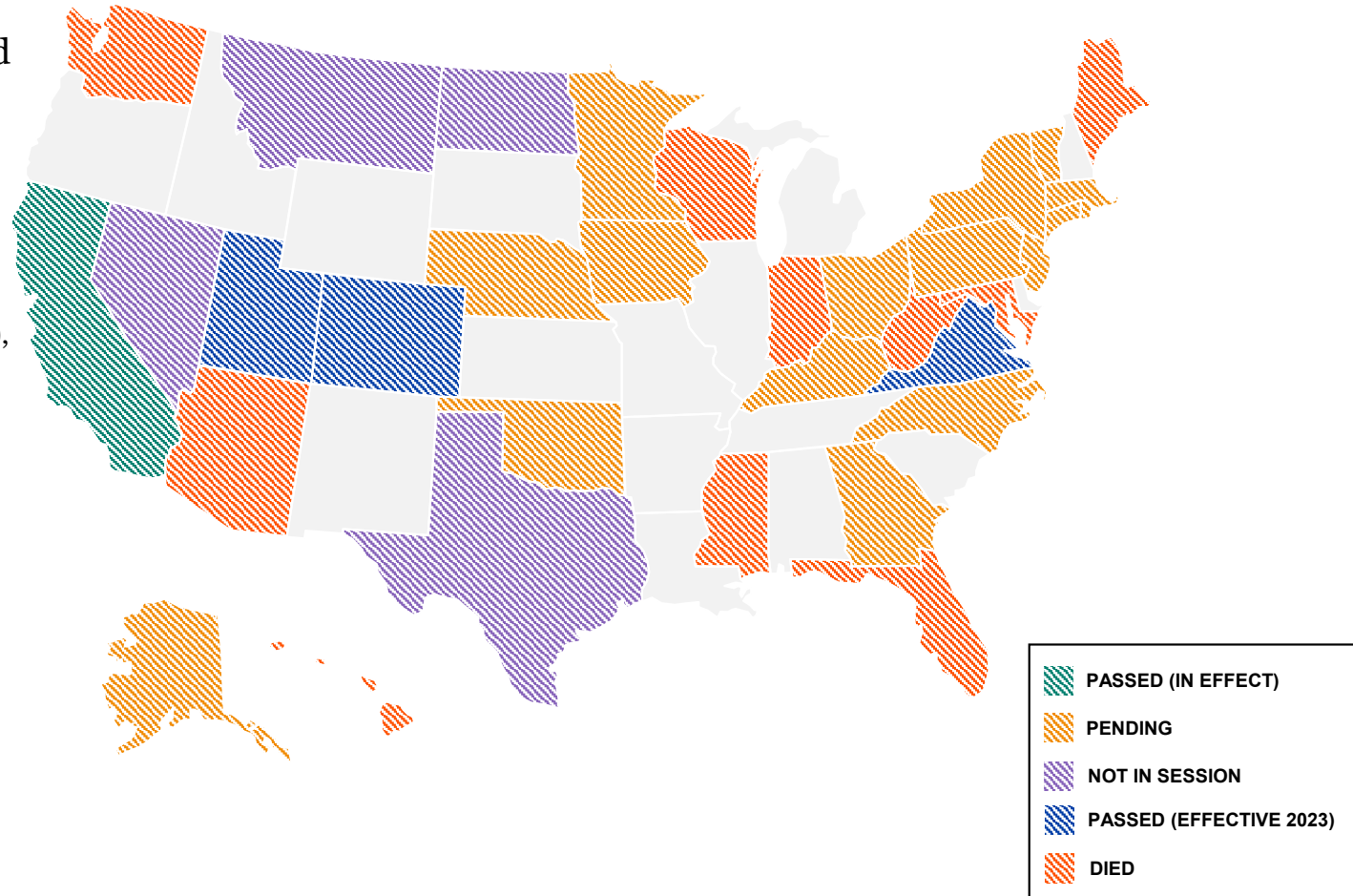
## Pending Legislation

- 27 states over 3 years
- Midwest Alert
  - MO (2022)
  - KY (2022)
  - IN (2022)
  - OK (2021)
  - WI (2019)

# Pending Legislation: Comprehensive Bills

## New Bills

- 29 states & 50+ bills introduced
- 1 signed (UT)
- 2 cross chamber
  - OK (2x)
- 29 in committee
  - AK (3x), CT, DC, IA, KY (2x), MA (2x), NE, NJ (3x), NY (5x), NC, OH, OK, PA (3x), RI (2x), VT (2x)
- 23 died in committee
  - AZ, FL, HI (4x), IA, IN, ME, MA (3x), MI, MN, MS, WA (4x), WV, WI (4x)
- 4 died after passing one chamber
  - FL, IA, IN, WI
- 1 converted to “work group” (MD)



# Trends

- Business friendly (modified Virginia)
- Government enforcement with right to cure
- Consumer rights
  - **Common:** access, sales opt-out
  - **Less common:** correction, portability, restrict profiling/targeting
  - **Rare:** private right of action
- Business rights/obligation
  - **Common:** transparency & processing limitations
  - **Less common:** opt-in for selling minor data
  - **Rare:** risk assessments; opt-in for selling sensitive data

# Midwest Trends

- Standard privacy fare [IA, IN, MN, NE, OH, OK, WI]
- Notable silence [KS, IL, MI, MO]
- Uniform law commission proposal [NE, OK]
  - Provides limited consumer rights
  - Allows “compatible data practices”
  - Permits pay-for-privacy
  - Exempts behavioral advertising



# Things to Watch

- Bills, Bills, Bills
  - Right to cure
  - Private right of action
  - Rulemaking authority
  - CPRA vs. CPA vs. VCDPA
- Rulemaking in Colorado and California
- FTC Advanced Notice of Proposed Rule Making on privacy & algorithms

# 2022 Legislation: Rights Comparison

Right	Description	Bills with Right
Access	Right to obtain from Controller certain details about the PI	98%
Correction	Right to request correction of incorrect/outdated PI	78%
Deletion	Right to request deletion of PI	89%
Restrict Processing	Right to limit the processing of the PI	20% [but 40% limit to profiling and targeted ads]
Portability	Right to request copy of PI in portable format	73%
Limit Sales	Right to opt out of having your PI sold or requirement that user opt in before Controller can sell the data	74% Opt-Out and 21% Opt-In
Automated Decision Making	Right to prevent using PI to make decisions about a person using automated means without any human intervention	19% [but 33% have limited right]
Private Right of Action	Right for consumer to sue a business for violating the privacy bill	31% [but 18% have limited right]

# 2022 Legislation: Obligations Comparison


Obligation	Description	Bills with Obligation
Obtain Opt-In Consent for Sale (consumer age)	Prohibits selling PI of consumers under a certain age, unless consumer opts-in	72% [excludes states requiring opt in for all data]
Obtain Opt-In Consent for Sale (data type)	Prohibits selling sensitive PI unless consumer opts-in	37% [excludes states requiring opt in for all data]
Transparency	Requirement to provide consumers notice about certain practices	100%
Risk Assessments	Requirement to conduct risk assessment of certain activities	41% [7% require in narrower situations]
Discrimination	Prohibits discriminating against consumer who exercises their rights	93%
Processing Limits	Prohibits processing PI except for specific purpose	82%



# Cybersecurity Risks and Preparedness



# Wait. How Much?




**\$4.24M**

GLOBAL AVERAGE TOTAL  
COST OF A DATA BREACH



**\$4.62M**

AVERAGE TOTAL COST OF A  
RANSOMWARE INCIDENT



**\$9.23M**

AVERAGE COST OF A  
HEALTHCARE DATA BREACH



**\$1.59M**

LOST BUSINESS COST



**287**

AVERAGE DAYS TO IDENTIFY +  
CONTAIN A COMPROMISE



**54.9%**

COST REDUCTION WITH  
INCIDENT-RESPONSE  
PROCEDURES IN PLACE

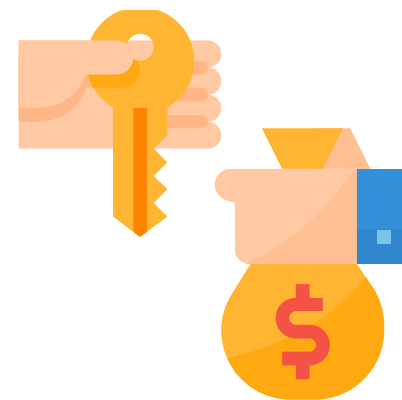


The average total cost gap between **IR capabilities vs. no IR capabilities** was **\$2.46 million in 2021, representing a 54.9% difference.**

IBM Security/Ponemon Institute, Cost of a Data Breach Report 2021

# Ransomware Basics

- Exfiltration and encryption
- Ransomware-as-a-Service
- Well-known groups
  - Conti
  - Lockbit
  - Zeppelin
  - \_\_Locker
  - REvil (??)



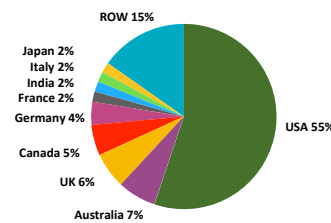


# Global Ransomware Threat

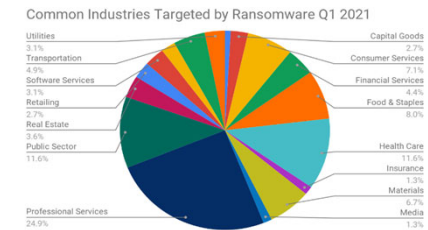
## Key Trends

- 83.3% of attacks threatened data exfiltration
- Median size of victims is below 150 employees (and shrinking)
- 78.3% of attacks target companies under 1,000 people
- Average businesses faces 22 days of interruptions due to an attack
- The cost of ransomware remediation has more than doubled (to \$1.85 million) in the last year

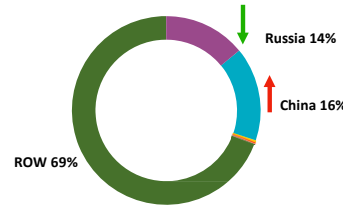
### Attacks by Country



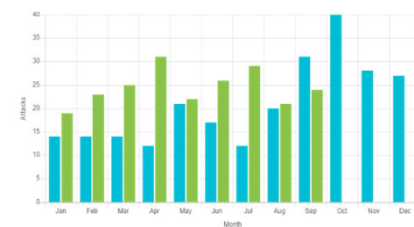
### Attacks by Industry



### Ransomware Exfiltration

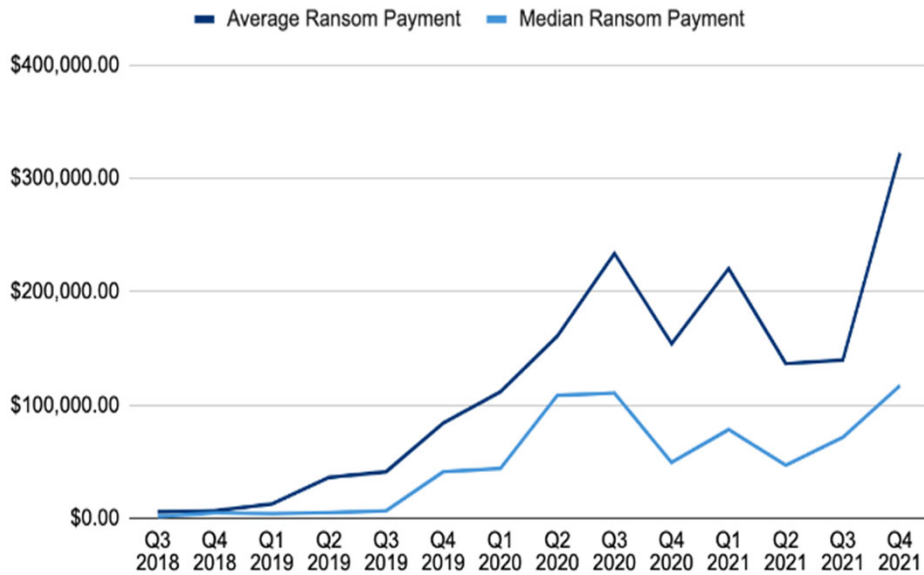


### Attack Trend by Month

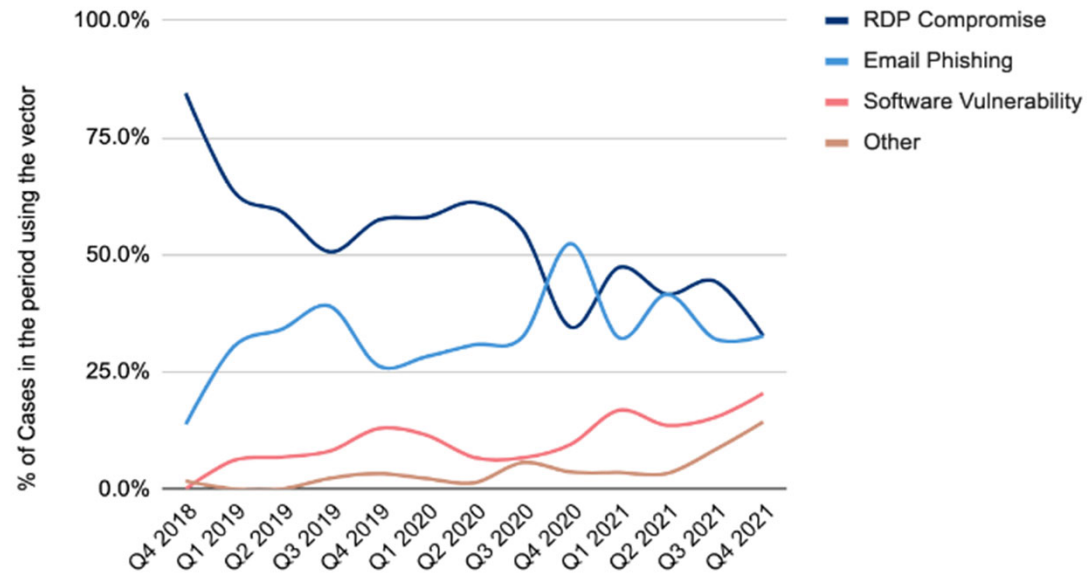


# Coveware Q4 2021 Ransomware

Ransom Payments By Quarter



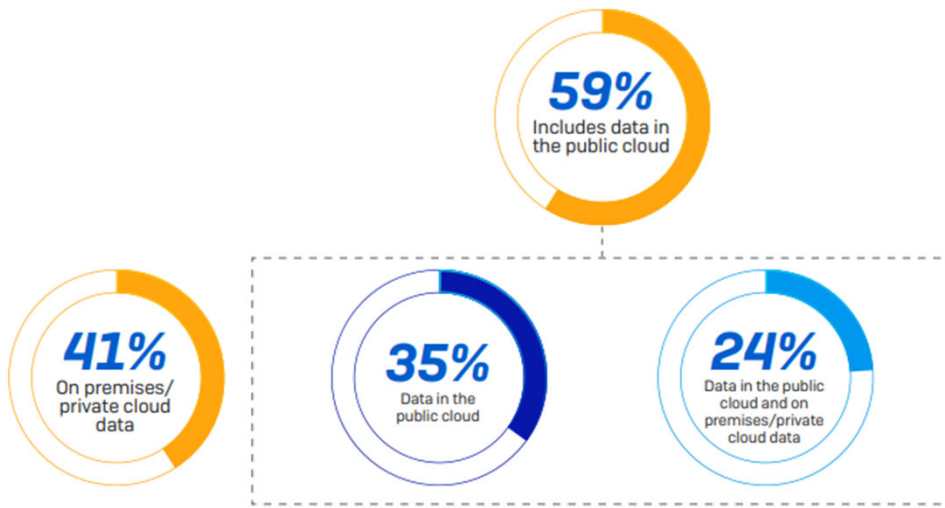
Ransomware Attack Vectors



Source: <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>

# Data Locations + Retrieval

## LOCATIONS OF AFFECTED DATA



## DATA RETRIEVAL AND RECOVERY

2020	2021	
26%	32%	Paid ransom to get data back
56%	57%	Used backups to get data back
12%	8%	Used other means to get data back
94%	96%	Total that got data back



# POLL

# Business Email Compromise

- What is a business email compromise?
- How does it originate?
- What to expect –
  - First 24 hours
  - First week
  - First month



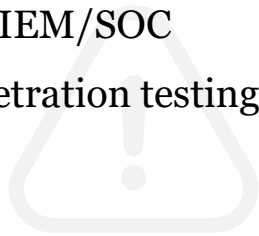
# Legal Issues to Consider

- Notifying insurer
- How to engage a forensic firm to maximize privilege
- Ransomware - whether to pay the ransom
- Whether the incident is a notifiable event, who to notify, and when
- Liability created by statements to employees and public
- Evaluating potential third-party liability/indemnification
- Cyber insurance coverage/exclusions

# Cybersecurity Preparedness

## THREAT MONITORING + RESPONSE

- Firewalls
- AV, EDR, DLP
- Regular vulnerability scans
- **Email filtering and phishing tests**
- Monitored SIEM/SOC
- Regular penetration testing



## ASSET MANAGEMENT

- **Patch management**
- Mobile device management
- Asset hardening



## ACCESS CONTROL

- **Multi-factor authentication**
- Privilege restrictions
- Minimum password complexity or secure passphrases



# Cybersecurity Preparedness

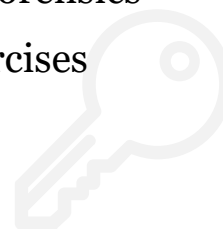
## SECURE STORAGE

- **Multiple layers of backups**, including air-gapped, on-prem, and cloud
- **Encryption at rest**
- Encrypted mobile storage devices
- Secure email option



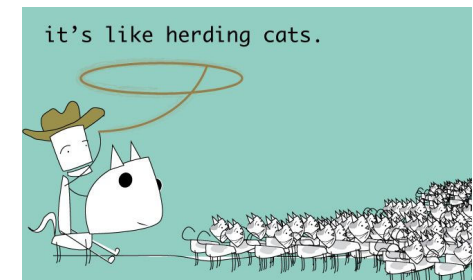
## INCIDENT RESPONSE

- **IRP** regularly reviewed and updated
- **Cyber Insurance**
- Established relationships with outside counsel and forensics
- Tabletop exercises



## PERSONNEL MANAGEMENT

- **Annual training** and policy acceptance
- Access control







Q + A

The logo for SHOOK HARDY & BACON is centered on a dark blue background with a subtle grid pattern. The word "SHOOK" is in a large, white, sans-serif font, with a thin orange horizontal line underlining the "OO". Below it, "HARDY & BACON" is written in a smaller, white, sans-serif font.

SHOOK  
HARDY & BACON

PRIVILEGED AND CONFIDENTIAL