HEALTH / SCIENCE / TECHNOLOGY
Critical in a crisis, creative in court.®
/ SHB.COM /

AUGUST 19,2021

Why Data Privacy Laws Could Crush Your Business

Presented By | Al Saikali, Chair, Privacy & Data Security Practice

SHOOK
HARDY & BACON

Overview

1. Whatever You Want
2. Session Replay Litigation
3. Lessons from HB 969
4. Biometric Privacy Laws
5. Ransom Payments

Anything You Want To Discuss

Discussion

- How important is consumer data to you?
- Why is it important?
- Who can tell us what the word “analytics” means?

What You Will Learn

- The private right of action for statutory damages can crush your company.
- The cost of compliance is expensive.
- Bad guys are finding new ways to make money off your data.

“Session Replay Litigation”

Session Replay Software

- Small pieces of code that, together, replay a user's visit to a website.
- Companies use it to:
  - improve user experience on website;
  - identify and address technical issues;
  - identify ways to improve conversion.
- Some providers offer "privacy by design" which limits what the customer can see about the user.
- The session replay files are large, so the retention periods are short, and it's expensive to store recordings.

The Florida Security of Communications Act

- Florida's wiretap statute.
- Prohibits the interception of electronic communications.
- Electronic communication means any transfer of data transmitted by a wire that affects intrastate commerce.

The FSCA's Private Right of Action

- Creates a private right of action in which plaintiff can recover:
  - Equitable relief;
  - Actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day or violation or $1,000, whichever is higher;
  - Punitive damages; and
  - Attorney's fees and costs (one way)

Litigation Landscape

- More than 50 lawsuits filed in Florida the last three months.
- Defendants include Banana Republic, Intel, Nieman Marcus, Adidas, The Gap, Spirit Airlines, and General Motors.
- Lawsuits filed in state courts throughout Florida (“shotgun approach”).

State Privacy Law Trends: Lessons from HB 969

HB 969

- Scope
  - Greater than $25M in annual revenue
  - Buy, receive, sell, or share personal information of 50k or more consumers, households, or devices
  - 50% or more of global revenue from selling or sharing personal information about consumers
- Personal Information (PI)
  - Any information that relates to a particular consumer or household or is reasonably capable of being associated with a particular consumer or household.

Examples of Personal Information

- Sensitive info (SSNs, DL#s, CC#s)
- Email address
- Protected classification info (Mr./Mrs.)
- Biometric information
- Internet or other electronic network activity (browsing history, search history, consumer's interaction with an Internet website, application, or advertisement)
- Geolocation
- Audio, visual, or olfactory information
- Professional/employment-related info
- Educational info
- Inferences drawn about a consumer's preferences, characteristics, behavior, abilities, and intelligence.

HB 969 Requirements (1 of 2)

- Maintain an **online privacy policy** and a **"just in time" privacy notice**
- **Provide a copy** of PI to consumer when requested
- Implement a **retention schedule** prohibiting use/retention of PI after initial purpose is satisfied or one year after consumer's last interaction with the business
- **Delete or correct PI** when requested by consumer
- **Right to know** what PI is sold or shared with third parties

HB 969 Requirements (2 of 2)

- Right to **opt out** of the sale or sharing of PI to third parties
- **Opt-in** requirement for the sale or sharing of information for minors under 16
- **Cannot discriminate** against consumers who exercise their privacy rights
- **Contract with third parties** with whom you share PI to limit their use of the PI
- Add a *"Do Not Sell or Share My Personal Information"* link to your website.

HB 969 Exceptions

- PI for employees, applicants, interns, or volunteers
- Health information, covered entities, and business associates under HIPAA
- PI governed by
  - the Fair Credit Reporting Act
  - the Gramm-Leach-Bliley Act
  - the Driver's Privacy Protection Act
  - the Family Educational Rights and Privacy Act

Why it would have been crushing

- Legal fees to understand and comply with the law - $50,000 to $200,000
- Data inventory - $40,000 to $120,000
- Solutions to keep the inventory evergreen - $40,000 to $200,000 per year
- Consultants to develop and implement a data subject access request process - $50,000 to $75,000

- Cybersecurity risk assessment - $25,000 to $130,000 per year
- Cyber insurance - $10,000 to $100,000 per year
- Training - $20,000 to $75,000 per year
- Hiring additional staff - $45,000 to $110,000 per year

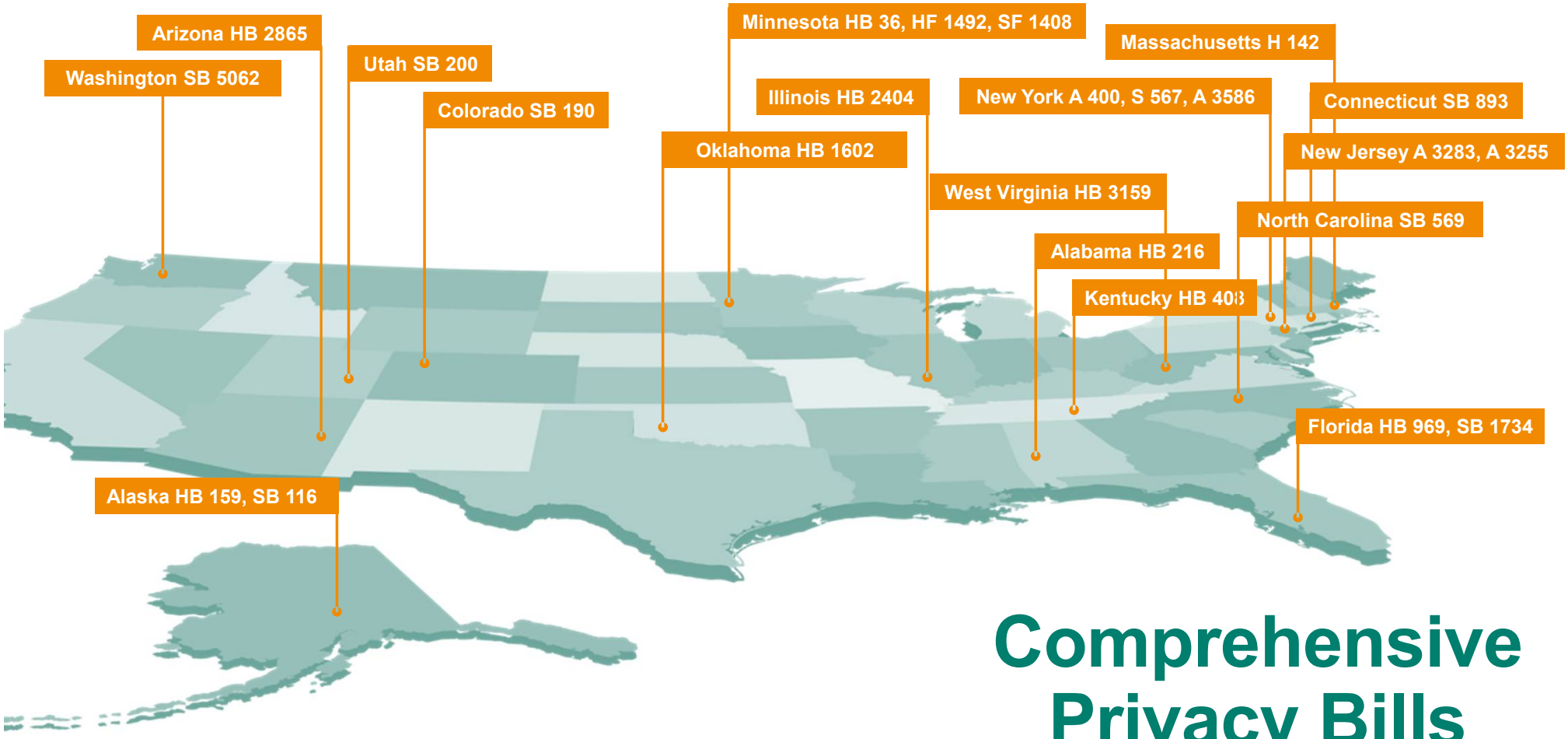
GRAND TOTAL = approximately **$300,000 to over $1 million**, most of which is not a one-time cost.

HB 969 Private Cause of Action

- If PI (broadly defined) is subject to a data breach and the business failed to implement and maintain reasonable security procedures and practices, the consumer can sue for:
  - Damages in the amount of $100 to $750 per consumer per incident
  - Injunctive or declaratory relief

HB 969 Private Cause of Action

- Consumers can also sue for those same damages if the business does not delete, correct, or execute opt-out as requested.
- The plaintiff can seek attorney's fees.
- Some examples
  - Data breach of meal preferences, allergy information, behavior
  - Incorrect statement in privacy notice
  - Failure to delete PI in backup files



Comprehensive Privacy Bills

(drawing on CCPA or GDPR)

Virginia Consumer Data Protection Act

- *Effective Jan. 1, 2023*
- "Personal data," "controller," "processor"
- Consumer rights
  - Confirm / access
  - Correct / Delete
  - Data minimization
  - Opt out of processing / consent to processing of sensitive data
  - Non-discrimination
- No private right of action

Biometric Privacy Laws: “BIPA”

BIPA's Requirements

- Applicable to **private entities**;
- Requires **notice** and **consent/release** before biometric identifiers or biometric information are **collected**, and a publicly-available policy re. **retention** and **destruction** for data **possessors**;
- Requires consent for **disclosure**;
- Must use **reasonable care** to safeguard/transmit;
- **Limits retention** to the purpose for its collection;
- Requires **destruction** when no longer needed.

What is a Biometric Identifier?

Biometric identifier: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."

Expressly does ***not*** include:

- Writing samples
- Written signatures
- Photographs
- Human biological samples used for valid scientific testing or screening
- Demographic information
- Tattoo descriptions
- Physical descriptions (*e.g.* height, weight)
- Certain information under the Illinois Anatomical Gift Act, the Genetic Information Privacy Act, and HIPAA.

The BIPA Private Right of Action

"Any **person aggrieved** by a violation of [BIPA] shall have a right of action," and "a prevailing party may recover **for each violation**."

- $1,000 (negligence) / $5,000 (intentional)
- Attorneys fees; costs; injunctive relief

Why It's Crushing – What BIPA Lawsuits Allege

- Employers violate BIPA by using finger or hand-scan timekeeping systems that allegedly collect biometrics, without advance notice/consent and retention/destruction policy
- Timekeeping technology providers violate BIPA for these same reasons;
- Consumer-facing cases against tech giants for same types of violations (Facebook "Tag Friends");
- Claim "per violation" damages of $1,000 or $5,000.
- Over 1,000 BIPA class actions have been filed.

Ransom Demands

What is Ransomware?

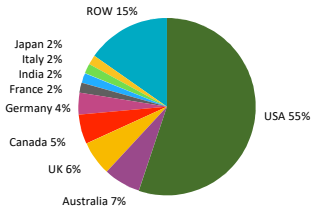
- Leveraging an existing vulnerability that usually encrypts data

- Threat actor demands a ransom for: (1) the decryption key; (2) deletion of your data; and/or (3) an agreement not to sell/distribute the data on the Dark Web.

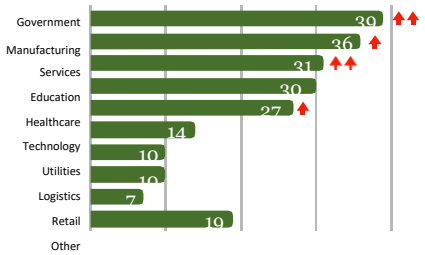
Global Ransomware Threat: January to November 2020

November was the third busiest month of the year with 28 attacks uncovered. Organizations in the **services industry** were hit the hardest, followed by the government sector. Education took a back seat this month with only one recorded incident. Here is a roundup of what we uncovered for the month.

Attacks by Country



Attacks by Industry



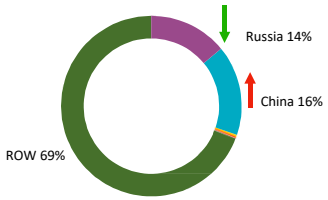
Key Trends

Average Ransomware Payment
$233,817 +31% From Q2

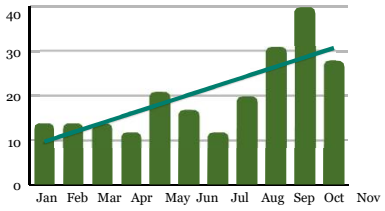
75% of all Attacks are Ransomware

80% of Attacks Exfiltrate Data

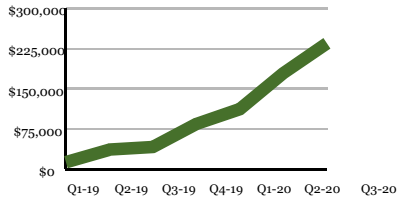
Ransomware Exfiltration



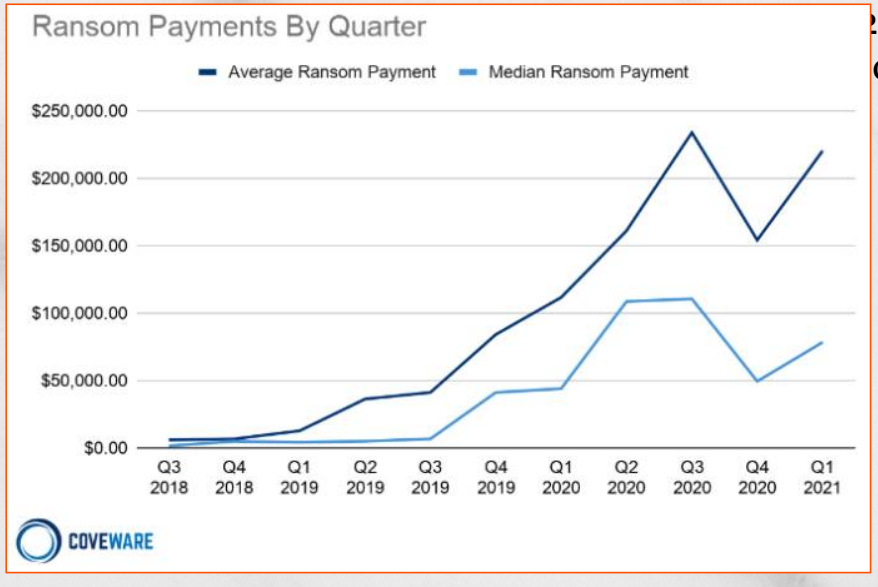
Attack Trend by Month

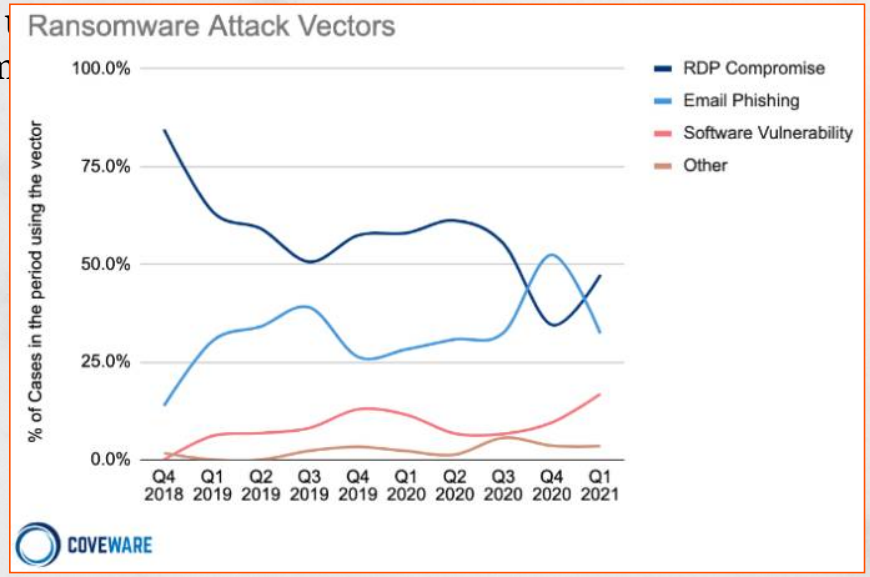


Average Ransom Payout[1]



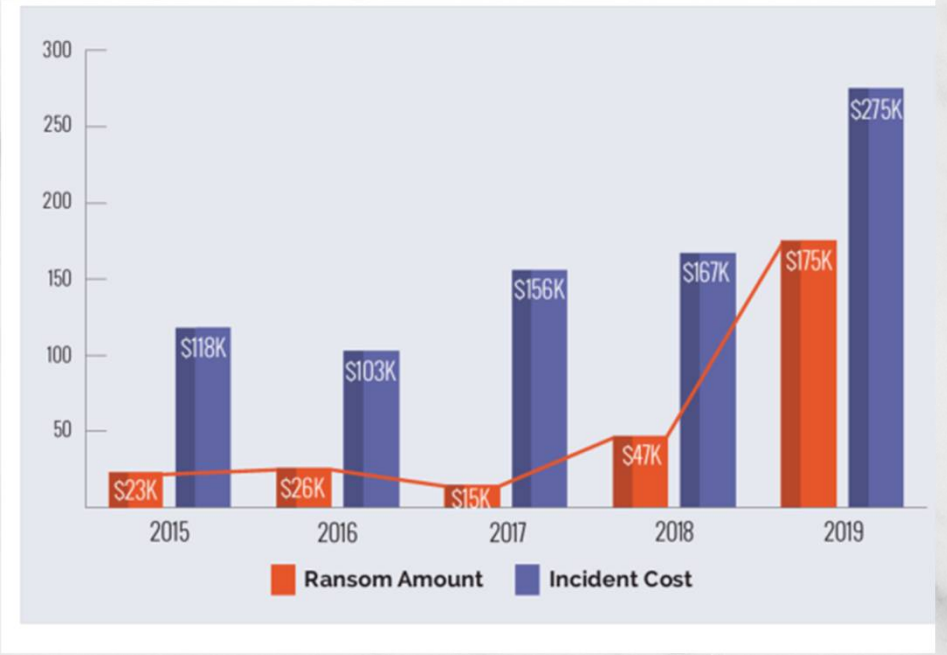
Coveware Q1 2021 Ransomware Report



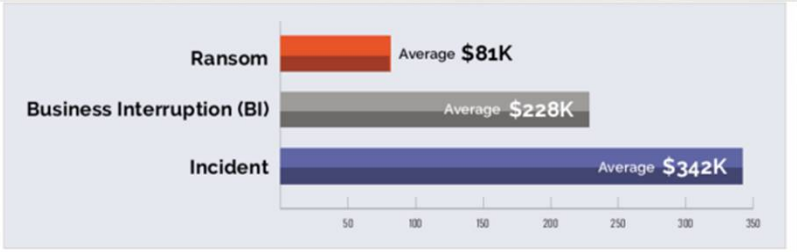


NetDiligence Cyber Claims (2020 Report)

Average Costs by Year



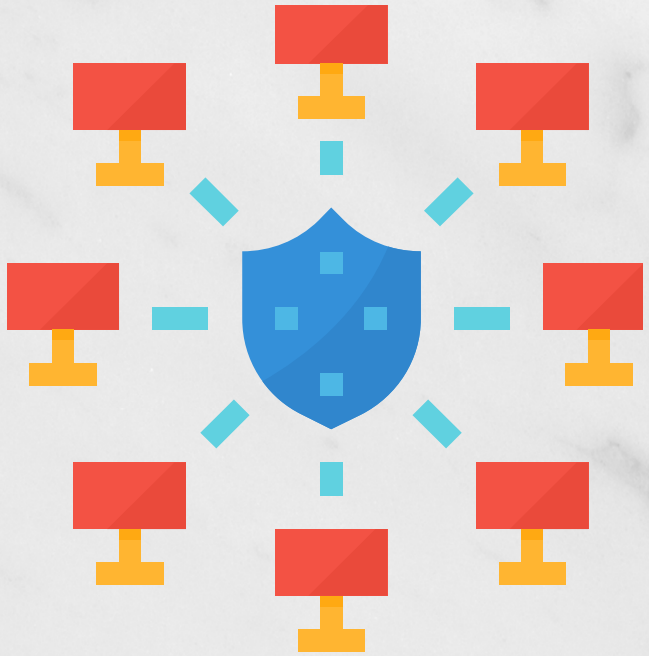
Ransomware that Include Business Interruption



Source: "Cyber Claims Study 2020 Report," NetDiligence, pg. 6 (2021)

How to Fix it (and why it's crushing)

- Secure backup
- Multifactor Authentication
- Regular third-party assessments
- Incident response plan
- Tabletop exercise
- Pay the ransom
- Cyber insurance



Questions? Thank you!

Al Saikali
Chair, Privacy & Data Security Practice
Shook Hardy & Bacon
(305) 960-6923
asaikali@shb.com

SHOOK
HARDY & BACON