

Cybersecurity and Privacy
Imperatives for WICPA
Business & Industry Spring Conference


Sarah A. Sargent | CIPP/US, CIPP/E, CIPM

March 16, 2022

GODFREY+KAHN MILWAUKEE | MADISON | GREEN BAY | APPLETON | WASHINGTON, D.C.

1

Today's Agenda



- ▶ The Current Threat Landscape
- ▶ Best Practices Pre- and Post-Breach
- ▶ Potential Legal Obligations After a Breach
- ▶ Privacy Imperatives to Be Aware Of

GODFREY+KAHN

2

The Current Threat Landscape

3

Russian Invasion of Ukraine Heightens Cyber Attack Risk

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

JOINT CYBERSECURITY ADVISOR Destructive Ransomware Targets Organizations in Ukraine

Russia-based ransomware group Conti issues warning to Kremlin foes

Conti ransomware gang's internal chats leaked online after declaring support for Russian invasion

Conti ransomware gang dismantles infrastructure amid Ukraine row

GODFREY+KAHN

4

Why Should Companies Care?

- ▶ For the first time in over five years, manufacturing companies were the most-attacked industry –23.2% of attacks in 2021
- ▶ This trend is expected to continue as many companies do not believe they are not a valuable target

GODFREY+KAHN

5

Why Should Companies Care?

- ▶ Significant Financial Costs of a Breach
 - ▷ Ransom
 - ▷ Lost business
 - ▷ Detection and mitigation
 - ▷ Notification obligations
 - ▷ Post breach response
- ▶ Global average total cost of a data breach: \$4.24m

GODFREY+KAHN

6

Key Statistics (2016-2020)

- ▶ Most Frequent Claims (SMEs)
 1. Ransomware (~1500, \$179,000 avg)
 2. Hacker (~450, \$430,000 avg)
 3. BEC (~400, \$123,000 avg)
 4. Phishing (~275, \$13,000 avg)
 5. Human Error (~250, \$72,000 avg)



Source: 2021 Intelligence Cyber Claims Report GODFREY+KAHN

7

Companies Can Be Vulnerable

Attack Vectors

- ▶ Physical Security
- ▶ Phishing
- ▶ Social Engineering
- ▶ Vendor Compromise

Attack Types

- ▶ Ransomware
- ▶ Email Compromise
- ▶ Wire Fraud
- ▶ Rogue employees



GODFREY+KAHN

8

Ransomware

- ▶ Malicious software
- ▶ Locks down a system and files making them inaccessible unless a ransom payment is made
- ▶ Can be accomplished through security vulnerabilities or phishing schemes



GODFREY+KAHN

9

Business Email Compromise

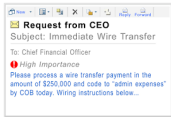
- ▶ Threat actor breaks into your email account
- ▶ Has access to entire inbox, can create rules to direct emails to folders so you have no idea
- ▶ Can send emails through your account without your knowledge
- ▶ Can be accomplished through security vulnerabilities or phishing schemes

GODFREY+KAHN

10

Wire Fraud

- ▶ Fraudulent wire instructions are communicated to parties through a business email compromise or phishing scheme
- ▶ A party unknowingly sends money to a threat actor



GODFREY+KAHN


11

Best Practices Pre- and Post-Breach

12

Best Practices Pre-Breach

- ▶ Be Prepared!
 - ▷ Written Information Security Plan (WISP)
 - ▷ Incident Response Plan
 - ▶ Tabletop Exercises
 - ▷ Engage data security and privacy counsel




GODFREY+KAHN

13

Best Practices Pre-Breach

- ▶ Data Minimization
 - ▷ If you don't need it, don't collect it
- ▶ Limit Access
 - ▷ Only those with a need to know should have access
- ▶ Emphasize Awareness
 - ▷ Employee Training




GODFREY+KAHN

14

Best Practices Pre-Breach

- ▶ Use technological measures to reduce the attack surface and mitigate common risks
 - ▷ Two-factor authentication
 - ▷ Encryption
 - ▷ Password managers like LastPass or strong passwords that vary across accounts



GODFREY+KAHN

15

Best Practices Pre-Breach

- ▶ Conduct vendor due diligence and use strong data security contractual provisions
 - ▷ Understand the measures a vendor uses to secure and keep private sensitive information
 - ▷ It is not sufficient to conduct due diligence at the outset, and never thereafter
 - ▷ Contractual provisions relating to reasonable security measures, data breach notification, reimbursement for notification expenses, and audit rights



GODFREY+KAHN

16

Best Practices Post-Breach

- ▶ Follow Incident Response Plan
- ▶ Take Action to Mitigate Harm if Possible
- ▶ Contact Insurer
- ▶ Contact Counsel
- ▶ Consider Attorney Client Protections when Working with Forensic Provider

GODFREY+KAHN

17

Potential Legal Obligations After A Breach

18

Breach Notification Laws

- ▶ Each state has its own data breach notification laws
- ▶ The definition of personal information may vary across states
- ▶ Each state will have its own standard for when notification is required
 - ▷ Access vs. Acquisition
 - ▷ Risk of harm
- ▶ Some states require notification of the state's Attorney General

GODFREY+KAHN

19

Wisconsin's Data Breach Notification Law—Wis. Stat. § 134.98

▶ Personal Information means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:



- ▶ The individual's Social Security number.
- ▶ The individual's driver's license number or state identification number.
- ▶ The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
- ▶ The individual's DNA profile.
- ▶ The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

GODFREY+KAHN

20

Wisconsin's Data Breach Notification Law—Wis. Stat. § 134.98

- ▶ Notice is not required if "the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information."
- ▶ Notice to be provided within a reasonable time, not to exceed 45 days after learning of the incident.

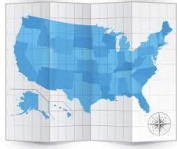


GODFREY+KAHN

21

Breach Notification Laws

- ▶ You will need to do an analysis of every state's law in which an affected individual resides



GODFREY+KAHN

22

Privacy Imperatives To Be Aware Of

23

What Are Privacy Laws?



- ▶ Laws that govern how a business may collect, use, and store personally identifiable information.
- ▶ Includes requirements for what a business must tell individuals about the collection of their information.
- ▶ In the U.S., these laws vary by state or sector.

GODFREY+KAHN

24

What is Personally Identifiable Information?



- ▶ There are different definitions used depending on the law or regulation.
- ▶ Generally, it is any information that can be used to identify an individual.
- ▶ For example:
 - ▷ SSN, name, address, driver's license number, passport number, financial account information

GODFREY+KAHN

25

Do Privacy Laws Apply to Your Business?

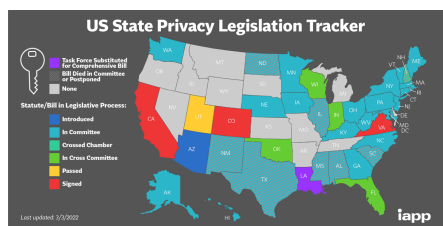


- ▶ In the U.S., currently three states have generally applicable laws on the books.
- ▶ Each state has their own applicability requirements.
- ▶ If you have international sales or employees, foreign privacy laws may apply, such as the EU's General Data Protection Regulation.

GODFREY+KAHN

26

Data Privacy is a Constantly Evolving Area of Governance in the U.S.



GODFREY+KAHN

27

U.S. Privacy Laws

VCDPA	CCPA	CPRA	CPA
Effective 1/1/23	Effective 1/1/20	Effective 1/1/23	Effective 7/1/23
Applies to businesses that:	Applies to businesses that:	Applies to businesses that:	Applies to businesses that:
<ul style="list-style-type: none"> Control/process PI of ≥25K consumers and derive 50% of gross revenue from sale of PI. Control/process PI of ≥100K consumers per year 	<ul style="list-style-type: none"> >\$25M annual revenue. Buy/sell/share PI of ≥50k households or CA residents. Derive 50%+ of annual revenue from selling PI of CA residents 	<ul style="list-style-type: none"> >\$25M annual revenue. Buy/sell/share PI of ≥100K CA consumers or households, or Derive 50%+ of annual revenue from selling or sharing PI of CA residents 	<ul style="list-style-type: none"> Control/Process PI of ≥100K consumers per Year. Derive revenue or receive discounts from the sale of PI and control/process data of ≥25K consumers

GODFREY+KAHN

28

Enforcement of U.S. Privacy Laws

VCDPA	CCPA	CPRA	CPA
Attorney General enforcement with 30-day cure period	Attorney General enforcement with 30-day cure period	Adds California Privacy Protection Agency enforcement	Attorney General enforcement with 60-day cure period
Penalties include injunction and up to \$7500 for each violation	Penalties include injunction and up to \$2500/ \$7500 for each violation Private right of action for data breaches caused by poor security	Removes cure period	Penalties include \$20,000 per violation

GODFREY+KAHN

29

Best Practices for Monitoring Privacy Laws

- ▶ Watch for developments in states where you do business
- ▶ Understand what data you do have that may be subject to these laws
- ▶ Work with legal counsel to understand obligations

GODFREY+KAHN

30

GODFREY & KAHN
MILWAUKEE | MADISON | GREEN BAY | APPLETON | WASHINGTON, D.C.

Thank You!



Sarah A. Sargent
414.287.9450
ssargent@gklaw.com

This presentation is intended to provide information on legal issues and should not be construed as legal advice. In addition, attendance at a Godfrey & Kahn, S.C. presentation does not create an attorney-client relationship. Please contact the speaker if you have any questions concerning the information discussed during this presentation.
