Navigating Cybersecurity:
Ransomware, the SEC Cybersecurity Rule, and More!

Kate Campbell, Godfrey & Kahn | CIPP/US, CIPP/E, CIPM
Lillie Conrad, 3M | CIPP/US, CIPP/E, CIPM

October 6, 2023

Disclaimer:

1. This material is for general information purposes only and should not be construed as legal advice or any other advice on any specific facts or circumstances.
2. No one should act or refrain from acting based upon any information herein without seeking professional legal advice. Godfrey & Kahn makes no warranties, representations, or claims of any kind concerning the content herein. Godfrey & Kahn and the contributing presenters or authors expressly disclaim all liability to any person in respect of the consequences of anything done or not done in reliance upon the use of contents included herein.

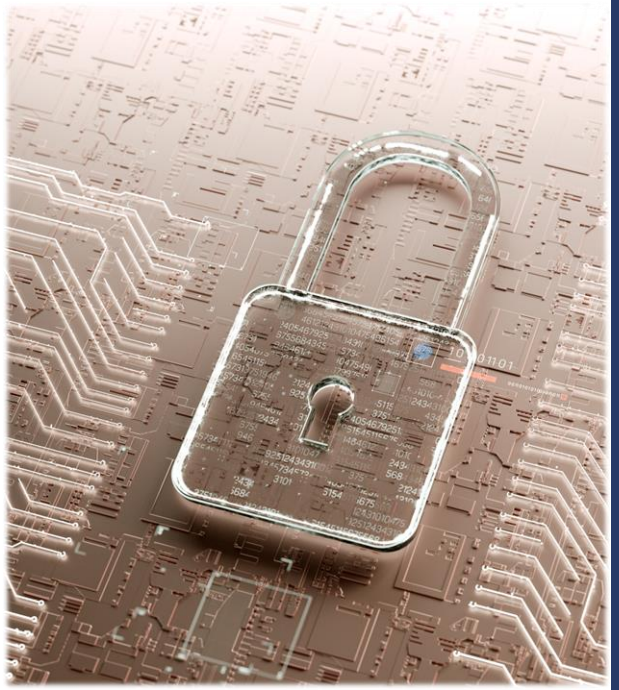
Today's Agenda

- The Current Threat Landscape
- Legal Obligations
- Best Practices Pre- and Post-Breach
- Practical Pointers for Effecting Best Practices

The Current Threat Landscape

Why Should Your Organization Care?

- Any company with data is an attractive target
- Significant exposure and exponential losses
- Volumes of sensitive information
- Legal obligations



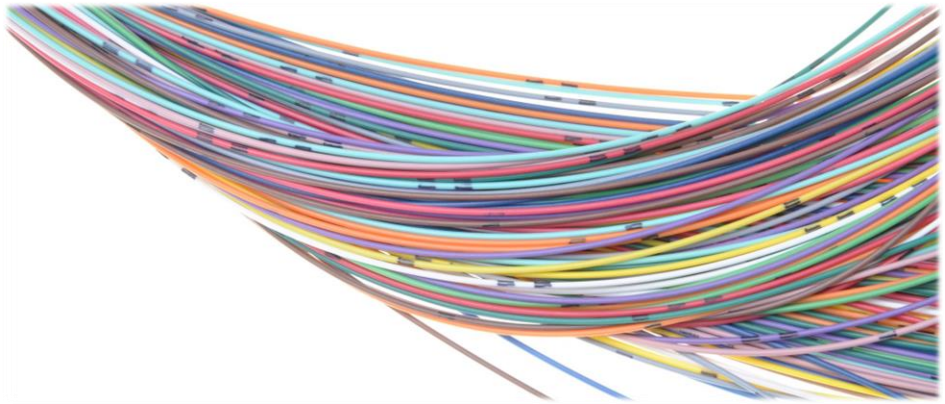
Vulnerabilities

Attack Vectors

- Physical Security
- Phishing
- Social Engineering
- Vendor Compromise

Attack Types

- Ransomware
- Email Compromise
- Wire Fraud
- Rogue employees



Ransomware

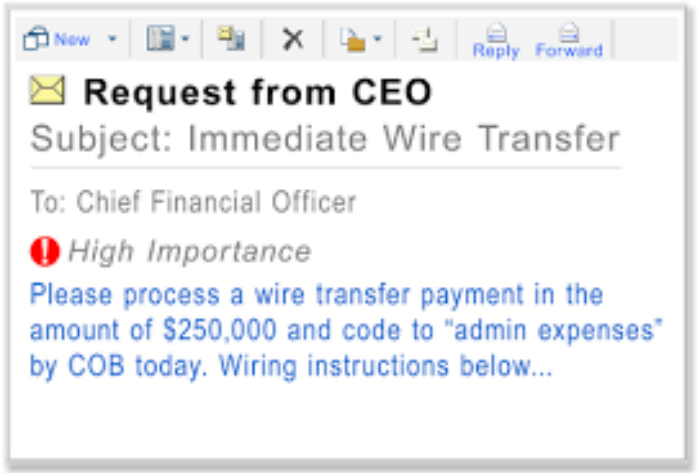
- Malicious software
- Locks down a system and files making them inaccessible unless a ransom payment is made
- Can be accomplished through security vulnerabilities or phishing schemes

Business Email Compromise

- Threat actor breaks into your email account
- Has access to entire inbox, can create rules to direct emails to folders so it isn't readily visible to you
- Can send emails through your account without your knowledge
- Can be accomplished through security vulnerabilities or phishing schemes

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



Evolving Threat Landscape

- Double and triple extortion models
- Top 5 most targeted industries: Government, Technology, Healthcare, Education and Financial Services

Key Statistics

- Average Incident Cost is at an all-time high of $4.45 million
  - 2.3% increase from 2022
  - 15.3% increase from 2020
- Healthcare has highest expense (average $10.93 million)
- Financial Industry has second highest expense (average $5.90 million)
- Reputational damage, regulatory fines and litigation expenses can be significant

Source: 2023 IBM Cost of Data Breach Report

Legal Obligations

SEC Cybersecurity Rule

- **July 26, 2023**: the U.S. Securities and Exchange Commission (SEC) adopted cybersecurity rules requiring public companies to disclose:
  - **material cybersecurity incidents** experienced on a current report on Form 8-K generally within four business days after the company determines the incident is material; and
  - **material information regarding their cybersecurity risk management, strategy, and governance** in the annual report on Form 10-K each year.
- **Effective Dates:**
  - The new Form 10-K disclosures will be required beginning with annual reports for fiscal years ending on or after **December 15, 2023**.
  - The new Form 8-K disclosures will be required beginning **December 18, 2023**, with some relief for smaller reporting companies.

Form 8-K Disclosure

- New Item 1.05 of Form 8-K, which triggers disclosures if a company experiences a cybersecurity incident that the company determines to be material.
- The Form 8-K disclosure must **describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the company**, including its financial condition and results of operations.
- An affected company must make a materiality determination "without unreasonable delay after discovery."
- The Form 8-K itself is due within **four business days** after the company determines that a cybersecurity incident is material.
- The rules permit **delayed disclosure** in cases in which the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety.
- All companies *other than smaller reporting companies* must begin complying with these requirements on December 18, 2023. Smaller reporting companies must begin complying on June 15, 2024

Form 10-K Disclosure

- New Item 106 of Regulation S-K, which will generally require annual disclosure in a company's Form 10-K under a new Item 1C. "Cybersecurity" of Part I, on the following topics:
  - **Risk management and strategy:** Companies must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
  - **Governance:** Companies must also describe their board of directors' oversight of risks from cybersecurity threats, as well as management's role in assessing and managing material risks from cybersecurity threats.

Data 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
  - Unauthorized access to personal information
  - Unauthorized access to personal information PLUS risk of harm
- Timing and the necessity to also notify the state's Attorney General varies across state laws

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.

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.
- The Wisconsin Attorney General is not required to be notified.

Breach Notification Laws

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

Other Required Notifications

HIPAA OBLIGATIONS

THIRD PARTY CONTRACTS

Best Practices and Practical Pointers

Best Practices Pre-Breach

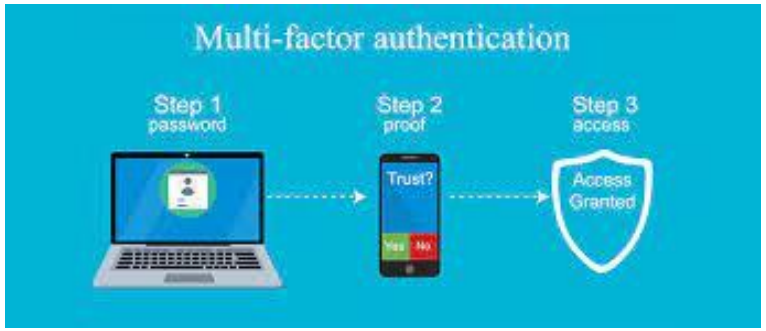
- Be Prepared!
  - Written Information Security Plan (WISP)
  - Incident Response Plan
    - Tabletop Exercises
  - Engage data security and privacy counsel

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

Best Practices Pre-Breach

- Use technological measures to reduce the attack surface and mitigate common risks
  - Multi-factor authentication
  - Encryption
  - Password managers like LastPass or strong passwords that vary across accounts
  - Email security
  - Endpoint Detection and Response



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

Cyberinsurance Tips

- Certain cybersecurity controls are critical to obtaining coverage:
  - Multi-factor authentication
  - Segmented, frequent, and encrypted backups
  - Prompt implementation of security patches/updates
  - Endpoint Detection and Response Tools
- Have a strong cybersecurity program in place and be knowledgeable about the security in place.
- Be thorough and truthful on your insurance application.

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