# Health Law Webinar

## Cybersecurity Basics:

## What Every Health Care Lawyer Should Know about Current Threats

**January 19, 2021**

Fredrikson & BYRON, P.A.

# Agenda

- Basic Cyber Vocabulary
- Ransomware – “So Hot Right Now”
- Business Email Compromises – Where Did the Money Go?
- Phishing – Exploiting the Weakest Link (Hint: It’s Your Employees)
- Special Considerations
  - Role of Counsel
  - Role of Insurance
  - Role of Law Enforcement

# Basic Cyber Vocabulary

# Personal Data “Breach” vs. “Incident

- **“Breach”** – an “incident” that results in the confirmed disclosure (not just potential disclosure) of personal data to an unauthorized party
- **“Incident”** – a security event that potentially compromises the integrity, confidentiality, or availability of an information asset (e.g., a device or system containing personal data)
- **Net/net**: just call it an incident

# “Exfiltration,” “Lateral Movement” and “Threat Actors” Oh My!

- **“Exfiltration”** –
  - Short version: data theft
  - Longer version: the unauthorized transfer of data from a company’s IT environment to a different, often unknown, location
- **“Lateral Movement”** – the techniques that a “threat actor” uses, after gaining initial access, to move deeper into a network
- **“Threat Actors”** – A/K/A cyber attackers, bad guys, evil doers, various four-letter words

# “Unauthorized Access” vs. “Unauthorized Acquisition”

- **“Unauthorized Access”** – an unauthorized person/entity has gained access to personal data without permission
- **“Unauthorized Acquisition”** – an unauthorized person/entity has exfiltrated personal data without permission

# Ransomware –
# “So Hot Right Now”

# Why Is Ransomware "So Hot Right Now?"

- $590 million in suspicious activity in first 6 months of 2021
  - Exceeded entire amount of 2020
  - Appx $102.3 million per month
- Several high-profile ransomware attacks
  - Colonial Pipeline
  - JBS
  - Kaseya

# What Is Ransomware?

- Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable
- A threat actor holds the data hostage until the ransom is paid
- If the ransom is not paid, the victim's data remains unavailable/unusable
- The threat actor may pressure victims to pay the ransom, or an additional ransom, by threatening to make the data publicly available

FBI Ransomware Fact Sheet (Feb. 4, 2021)

# What Is Ransomware (cont.)?

- Double ransom scenarios becoming the norm, with threat actor exfiltrating data before releasing the ransomware
- Threat actor may deny access to websites and harass victim's customers and employees
- Large ransom demands – avg. $1.2mm
- Hallmark of ransomware attack – sophistication
  - Serious criminal enterprises; sometimes state-sponsored
  - Concerned about reputation and, sometimes, "customer service"
  - Always leave multiple back doors into IT environment

# How Do Threat Actors Deploy Ransomware?

- **Phishing** – emails with a malicious file, link or website which deploy malware when clicked or visited
- **Remote Desktop Protocol Vulnerabilities** – RDP is proprietary network protocol that allow individuals to control resources and data of a computer over the internet. Threat actors try to exploit vulnerabilities and/or obtain credentials to gain unauthorized RDP access to victim's systems.
- **Software Vulnerabilities** – threat actors take advantage of weaknesses in widely used software programs to gain access to victim's systems

FBI Ransomware Fact Sheet (Feb. 4, 2021)

# Ransomware Attack – What Can You Expect?

- Initial compromise of your IT systems
- Reconnaissance and lateral movement through systems
- Identification of, and staging for exfiltration of, data
- Release of malware into environment
- Encryption of files
- Ransom demand

# Ransomware Attack – What Can You Expect (cont.)?

- Possible communications to employees and others by threat actor
- Inability to use encrypted aspects of IT environment

# Preparing for and Responding to Ransomware

Technical Tips

- Design IT systems to “assume compromise” – limit lateral movement
- Immutable backups – limit threat actor’s ability to encrypt backups
- Multi-factor authentication
- Apply updates/patches to IT systems
- Use solutions and enable logging that will allow visibility into activity conducted in environment
- Internal/external penetration testing
- More tips at https://www.cisa.gov/stopransomware/ransomware-guide

# Preparing for and Responding to Ransomware

Response Tips

- Develop an incident response plan with procedures for ransomware; test it
- Identify and train a cross-disciplinary internal response team
- Identify all external resources necessary in the event of a ransomware attack
  - IT forensics
  - Ransom negotiator; payment facilitator w/ bitcoin wallet
  - Outside counsel; crisis communications consultant
- Engage management on ransomware strategy

# Special Legal Consideration – Potential OFAC Violation

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

**Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments**[1]

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

OFAC issued guidance in Oct. 2020 and Sept. 2021 regarding enforcement action against entities that make or facilitate payments to individuals and entities on the embargo list

# Special Legal Consideration – Potential OFAC Violation

Key takeaways

- Ransomware groups and crypto currency exchanges are being included on the embargo list
- Payment of ransom demands to such groups, or using such exchanges, is prohibited
- Mitigating factors that OFAC will consider in enforcement activity include:
  - Strong cyber security practices
  - Notification and cooperation with U.S. government agencies, including prompt reporting of ransomware incidents, details regarding the incident and ransom demand and self-reporting of ransom payments
- Sept 2021 Guidance – https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

# Business Email Compromises – Where Did The Money Go?

# BECs are on the Rise/Costly


The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019:**

| | |
|---|---|
| Domestic and international incidents: | 166,349 |
| Domestic and international exposed dollar loss: | $26,201,775,589 |

# All Companies are Targets…

- BECs are not just a large company problem
  - According to the FBI's IC3 – "The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions."
- BECs are effective and widespread
  - "Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses."
  - "The scam has been reported in all 50 states and 177 countries."

# What is a BEC?

- BEC a/k/a “man-in-the-middle” or, more generically, “email account compromise” or funds transfer fraud
- Involves a threat actor compromising an employee’s (sometimes C-suite) email credentials and posing as the employee or another party in order to divert a payment stream or gain sensitive information
- Objective is typically financial – e.g., wire transfers, employee paycheck disbursements
- But not always. Threat actors may attempt to steal personal information – e.g., employee W-2s.

# What is a BEC? (cont.)

- The operative component of a BEC:
  - **Deception**
- BECs prey on individuals' innate desire to:
  - **Please / help**
  - **Succeed / not screw up**
  - **Mitigate stressful situations**

# Stages of a BEC

- Stage 1 – Research and investigation
  - BECs are not random
  - Threat actors may spend considerable time investigating an organization and targets within an organization
  - Both before and after the threat actor has compromised the organization's systems

# Stages of a BEC

- Stage 2 – Compromise / hacking
  - Email compromise
  - Domain impersonation – threat actor purchases a domain similar to the organization and nearly identical email account
  - Email spoofing – forged email address that appears to come from the target's email domain. No misspellings.
  - Targeted phone calls – Yes! The humble phone call can be an agent of social engineering.

# Stages of a BEC

- Stage 3 – Grooming
  - Threat actor, posing as legitimate individual (often C-suite), begins interacting with target
  - Threat may try to build up trust with the target and/or evaluate whether the target notices something is amiss
  - May occur over days or weeks
  - May use persuasion/pressure to coerce target

# Stages of a BEC

- Stage 4 – Payment request and payment
  - Threat actor makes a request for a funds transfer (or disclosure of personal information)
  - Target is convinced that it is a legitimate request
  - Target processes the request – funds are deposited in unauthorized account

# Stages of a BEC

- Stage 5 – Subsequent wire transfers
  - Initial transfer may be easily undone
  - Threat actors rely on multiple subsequent transfers to make tracing difficult
  - Frequently trying to get funds into international accounts
  - Threat actors use “money mules” to assist with laundering

# Sample BEC

From: managing.partner@fredlavv.com

To: associate@fredlaw.com

Re: ABC Co. v. DEF Co. Settlement

Associate,

I need you to provide the following wiring instructions to DEF Co. for the settlement payment:

Accountholder name: ABC 2 Co.

Account number: XXXXXXXXXXX

Routing number: XXXXXXXXXXX

The settlement payment is due tomorrow, so please provide these instructions to DEF Co. asap!

Thank you,

Managing Partner

# Keys to BEC Response

Fredrikson & BYRON, P.A.

# SPEED IS EVERYTHING

# Steps to Take in Response

1. **Notify the transferring bank**
   - Request a recall as soon as possible
2. **Notify the FBI**
   - File complaint on IC3.gov
   - Provide a copy to an agent / contact field office
   - FBI's Financial Fraud Kill Chain (if discovered within 72 hours of transfer)

# Steps to Take in Response

3. **Notify outside counsel**
   - Outside counsel can maintain privilege
   - May have contacts inside FBI
   - Should be part of incident response team
4. **Notify insurer**
   - Policy may cover BEC (many don't)
   - Policy may require law enforcement notification

# Steps to Take in Response

5. **Engage your incident response team**
   - Companies with incident response plans should convene IRT to coordinate response
6. **Engage additional IT support, if necessary**
   - Ensure you have the right resources to investigate and remediate any threats

# Preventing and Mitigating BECs

Fredrikson & BYRON, P.A.

# Prevention/Mitigation – Organizational Steps

- Train employees
- Encourage (appropriate) employee suspicion
- Develop secondary authorization procedures for payment requests
- Carefully scrutinize any payment requests that include a change in payment instructions
- Verify the changed instructions with client or vendor—but use known contact information (e.g., phone number)

# Prevention/Mitigation – Technical Steps

- Update your intrusion detection system
  - Consider rules that flag email addresses that are similar to the company's address
- Register similar domain names
- Develop an appropriate patching process for software and systems
- MFA for remote access

# Special Legal Considerations – Legal Liability

- Case law divergent
- Most courts follow the principle that losses arising from fraud should be paid for by the party in the best position to prevent the fraud
- If you were negligent, courts are likely going to hold you liable, at least in part, for any losses

# Phishing – Exploiting Your Weakest Link

# Why Does Phishing Matter?

- It is a building block for ransomware, BECs and other data security incidents
  - According to Verizon, 36% of the breaches in the data set it used to prepare its 2021 Data Breach Investigations Report involved phishing
- It is remarkably effective
  - Click rates vary by campaign, but KnowB4 conducted an analysis in 2021 that showed an overall phishing-prone percentage of 31.4%

# What Is Phishing?

- Phishing is the practice of sending fraudulent emails that appear to come from a legitimate source in order to induce the recipient to take some action
- The goal of phishing is typically to trick the recipient to either:
  - Hand over sensitive information, often an email username and password; or
  - Download malware onto their device, usually via an attachment or link

# Different Types of Phishing

- There are multiple different types of phishing. Some of the most common include:
  - Deceptive phishing – sending an email impersonating a legitimate entity or individual to steal someone's personal data or log in credentials
  - Spear phishing – purpose-built by the threat actor for the specific recipient
  - Whaling/CEO Fraud – Like spearphishing, but targeted at executive-level management
  - Vishing – Social engineering via phone
  - Smishing – Phishing via SMS text

# Strategies For Preventing and Mitigating Phishing

- The technical measures discussed previously apply equally to phishing
- Other technical and organizational measures:
  - Employee security awareness training
  - Mock phishing exercises (the more frequent, the more effective)
  - Develop and implement a password policy, with complexity and expiration requirements
  - Spam filters and anti-virus solutions
  - Web filters to block malicious websites
  - Encryption of sensitive data at rest and in transit

# Special Considerations

# Role of Counsel

- **Before an incident**
  - Coordinate and assist with incident response preparation
    - Develop and update the incident response plan
    - Identify and coordinate agreements with outside vendors
    - Conduct table-top exercises to test response
  - Understand the sensitive data types processed by the company and legal obligations applicable to such data in the event of a breach
  - Identify contractual obligations and develop processes for confirming reporting obligations in response to an incident

# Role of Counsel

- **During and after an incident**
  - Incident quarterback
  - Establishes incident investigation under privilege, to extent possible (see next slide)
  - Ensure appropriate chain of custody over forensic evidence is preserved, as appropriate
  - Review and coordinate timely notification per contractual obligations, to extent applicable
  - Review and coordinate timely notification per legal obligations (to affected individuals, regulators, etc.)
  - Coordinate post-incident review and change management

# Role of Counsel

- **Attorney-Client Privilege**
  - Increasingly difficult after decisions in *Capital One*, *Clark Hill*, and *Rutter's*
  - Factors helpful in establishing privilege
    - Outside counsel engages forensic vendor
    - Engagement is identified as necessary for outside counsel to provide legal advice
    - Any forensic report is limited to identify information necessary for legal advice
    - Disclosure of report and investigative findings is limited
    - Forensic vendor is paid from legal budget
    - Justifiable legal basis for any including any remedial measures identified in the forensic report

# Role of Insurance

- Coverages can include incident response expenses, first- and third-party losses, litigation fees, business interruption losses, ransom payments, funds lost to BECs, regulatory fines, etc.
- Typically dictate service providers and counsel to use in event of an incident
- Prompt reporting important for coverage
- Obtaining insurance increasingly difficult
  - Extensive underwriting analysis
  - Higher premiums
  - Higher retainers
  - Limited coverage for BECs

# Role of Law Enforcement

- FBI has publicly committed to “treat victim companies as victims”
- Should an entity notify?
  - Complex question
  - Pros:
    - Potentially invaluable information and assistance remediating the harm
    - May help others avoid harm
    - Improves optics/narrative
  - Cons:
    - Compelled participation w/ investigation
    - Information may be shared with regulators

# Parting Thought

# Questions?

# Presenter

**Sten-Erik Hoidal, CIPP/US**
Chair, Data Protection & Cybersecurity Group
612.492.7334
shoidal@fredlaw.com