



# Cybersecurity & Incident Response

## The Nuts & Bolts of Avoiding, Detecting and Responding to a Security Incident

State Bar of MI, HCLS Virtual Annual Meeting

September 23, 2021

# INTRODUCTIONS



Debra A. Geroux, JD, CHC, CHPC,  
Shareholder, Butzel Long



Scott Wrobel, Co-  
Owner, N1 Discovery

# AGENDA

- *Cyber risks in healthcare*: Update on what is trending in cyberattacks and risk areas
- *Incident response*: Real-world examples of how to handle cyberattacks
- *Federal Efforts to combat cyberattacks*: EO 14028 & CINA of 2021
- *Lessons learned* from recent cyberattacks
- *Best practices*

# New Cyber Facts & Statistics

- 70% of organizations experienced attacks in 2019
- Mobile malware variants increased by 54%
- New phish attacks release trojans
- Ransomware from phishing emails increased by 109% in 2019
- 80% increase in new malware on Macs
- Average user receives 16 malicious emails per month
- Increase in new ransomware variants: 46%

# More Healthcare Numbers in 2020

- 599 healthcare breaches
- affected more than 26 million people in 2020
- 91.2% of the records exposed as a result of hacking and IT incidents
- average cost per breach increased for healthcare organizations, from \$429 in 2019 to \$499 last year
- Data loss=\$13.2 billion in total

(Bitglass)

# Even More Statistics

- In 2018 the cybercrime cost to the Global economy was around \$600 Billion. In 2020 it was estimated to double (McAfee)
- Global spending on cyber security in 2020 is estimated at \$145 Billion (McAfee)
- US FBI Ic3 report indicated cybercrime complaints increased from 1000/daily (before COVID) to 4000/daily (during Covid) (McAfee)
- Confirmed healthcare data breaches increased 58% in 2020 (Verizon)
- Cloud-based cyber attacks rose 630% between January and April 2020. ([Fintech News](#))
- Average LOST Business \$1.52M (IBM) (Cf UHS posted a loss of \$67 due to 2020 ransomware attack)
- 30% of data breaches involve internal actors. ([Verizon](#))
- The average ransomware payment rose 33% in 2020 over 2019, to \$111,605. ([Fintech News](#))
- **HIGHEST ransomware increased 6-fold: increase in 2020 from \$5M to \$10M, recently a \$30M demand made**
- 94% of malware is delivered by email. ([CSO Online](#))

# Breaches Across the States in 2020

- 37 states suffered more breaches than the previous year, with California recording the most healthcare breach incidents at 49
- This was even higher than the 2019 record (43 incidents in Texas)
- Recovery from a breach took 236 days for the average healthcare firm last year

(Bitglass)



# Changes in Cyber Attacks

## *Well-funded, Smarter, Advanced, Patient*

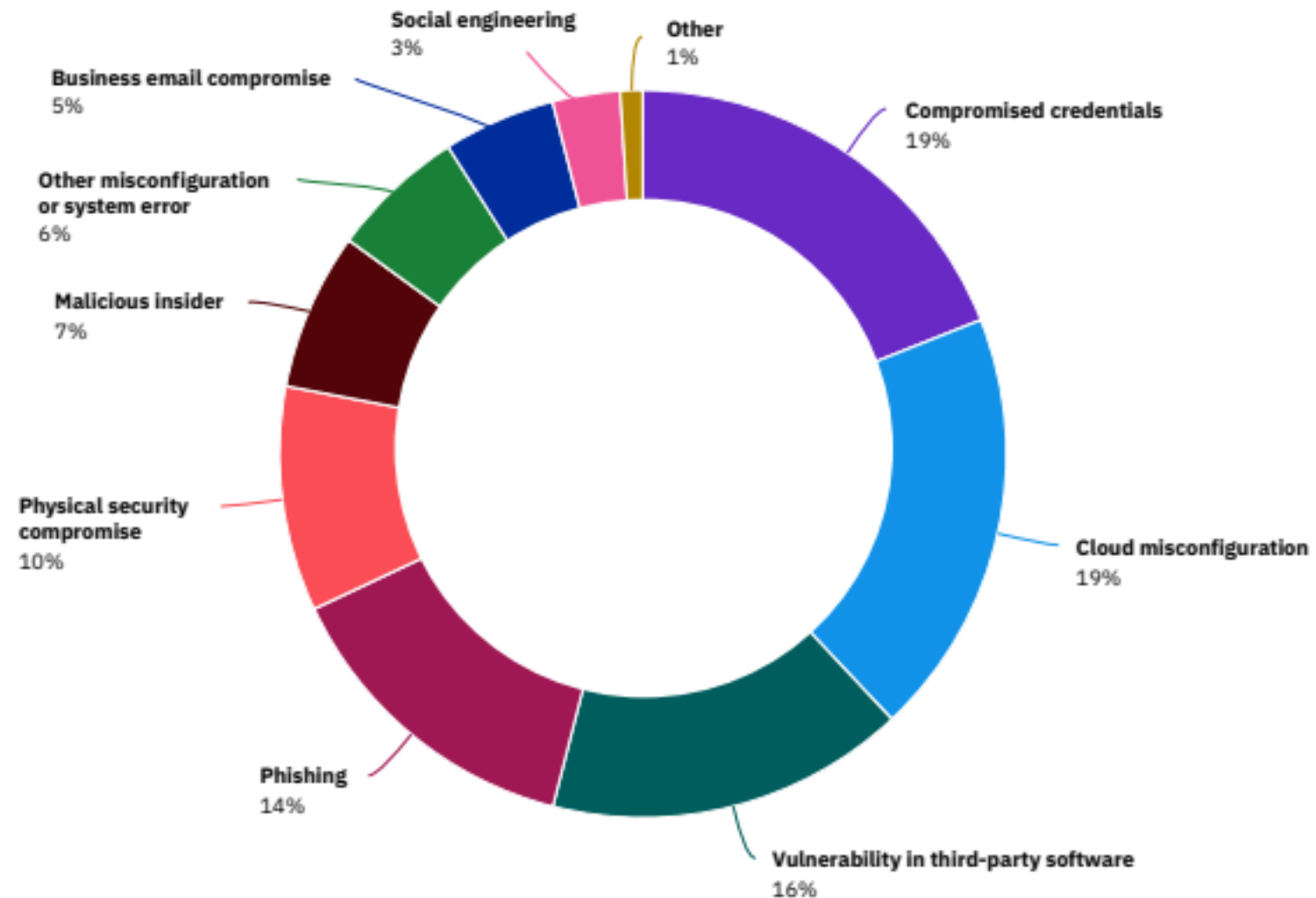
- Increased \$\$\$ in ransomware
- Educated, trained and experienced
- Sophisticated malware
- Thorough, diligent, patient
- Malware-as-a-service
- Ties to terrorist organizations



**Figure 21**

## Breakdown of malicious data breach root causes by threat vector

Percentage of breaches caused by malicious attack





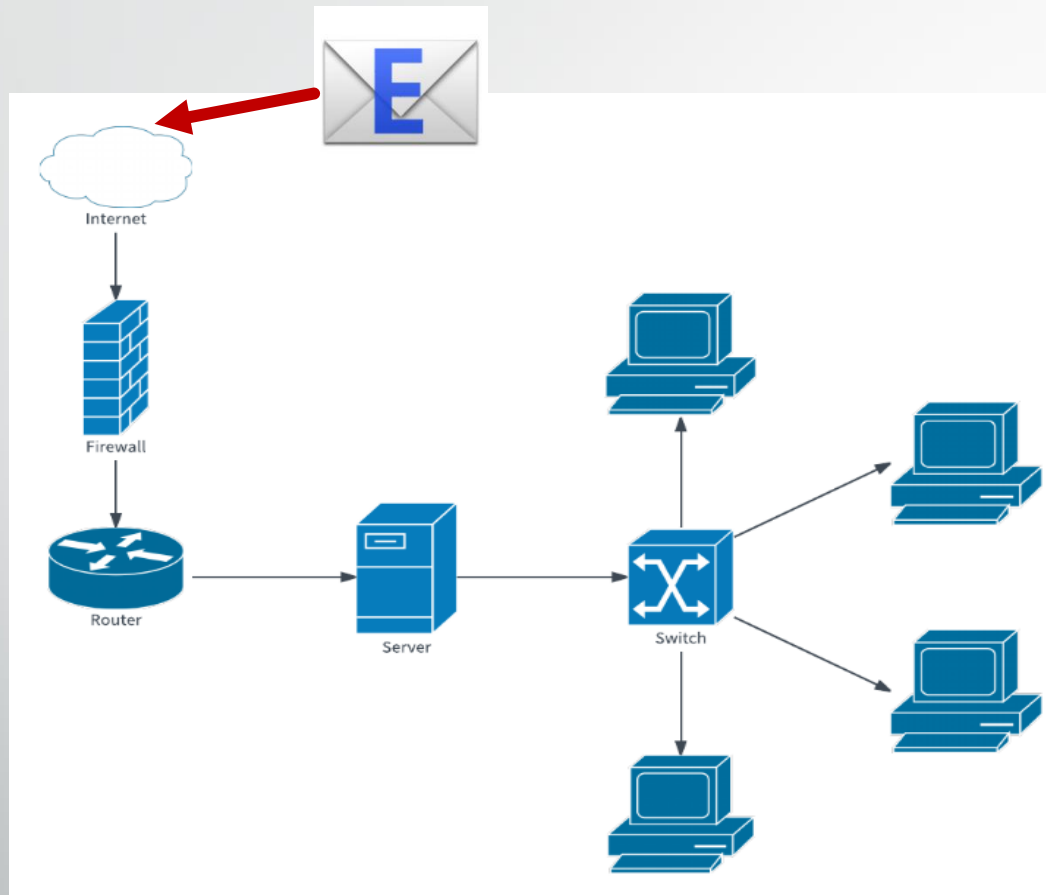
# Why is it Happening?



- Because it is profitable
- Products designed to make life easier
- Vulnerabilities in infrastructure
- Default settings
- Constant changes in technology (upgrades, patches)
- Easy access to malware
- **Human error**

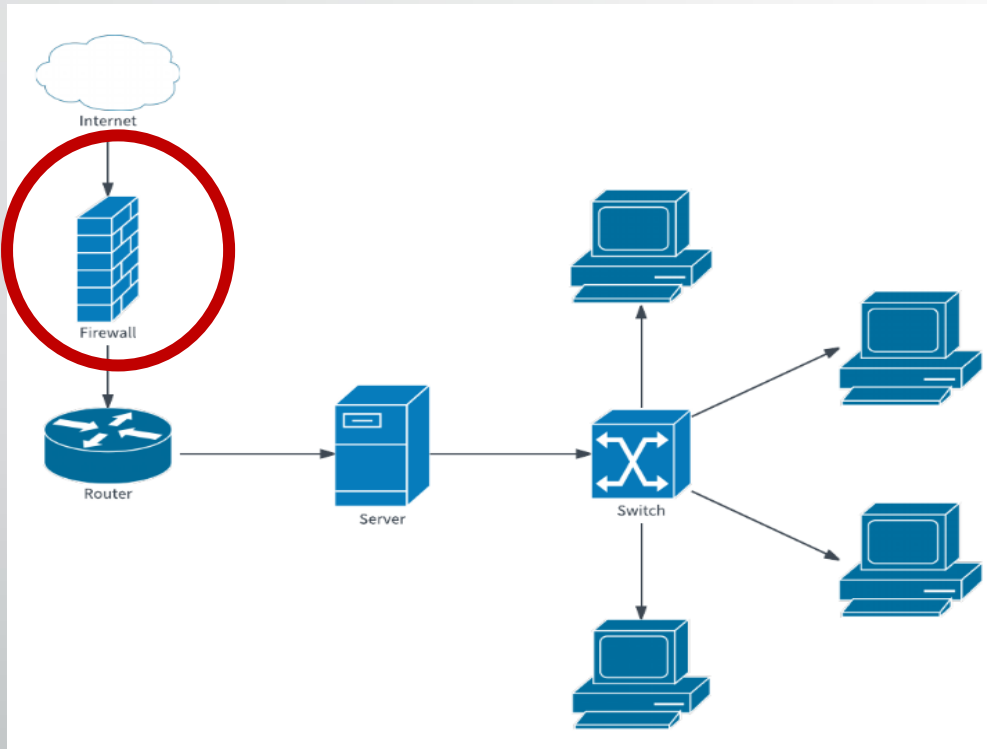


# How is it Happening?



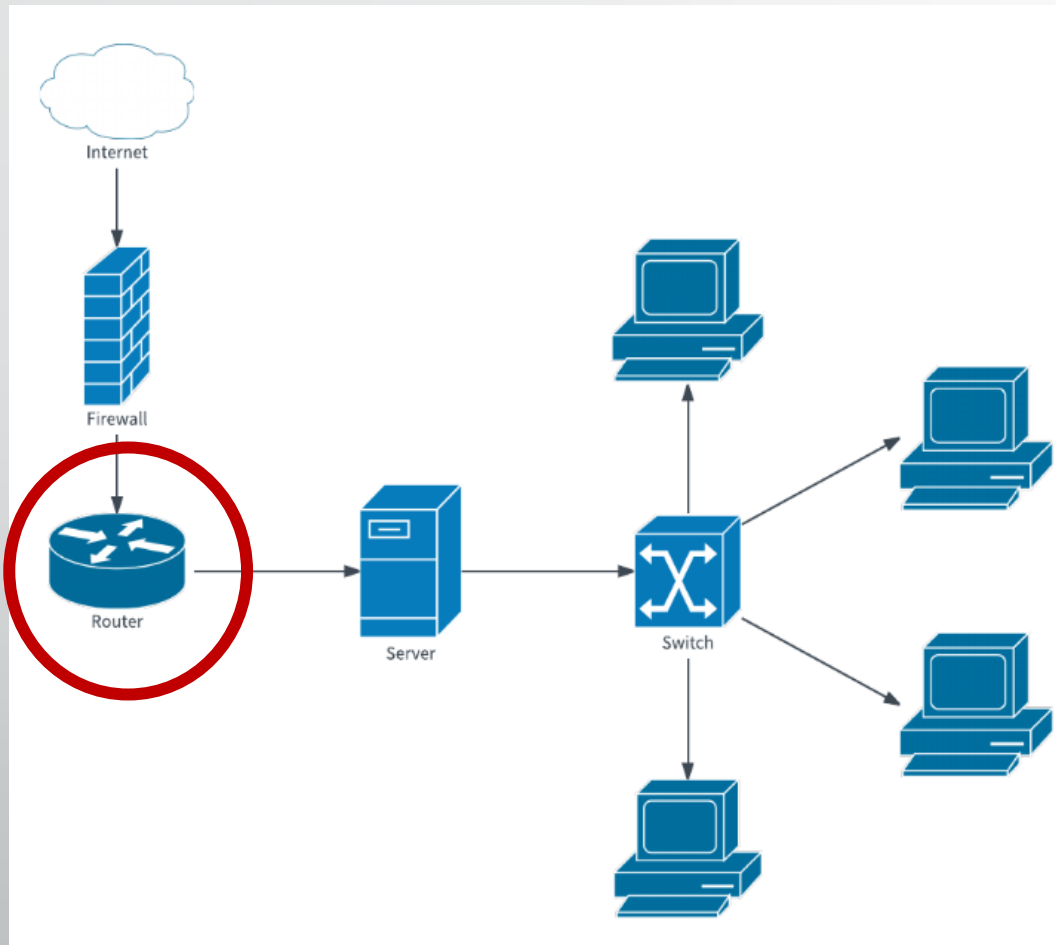
- Email
  - Office 365, default settings

# How is it Happening?



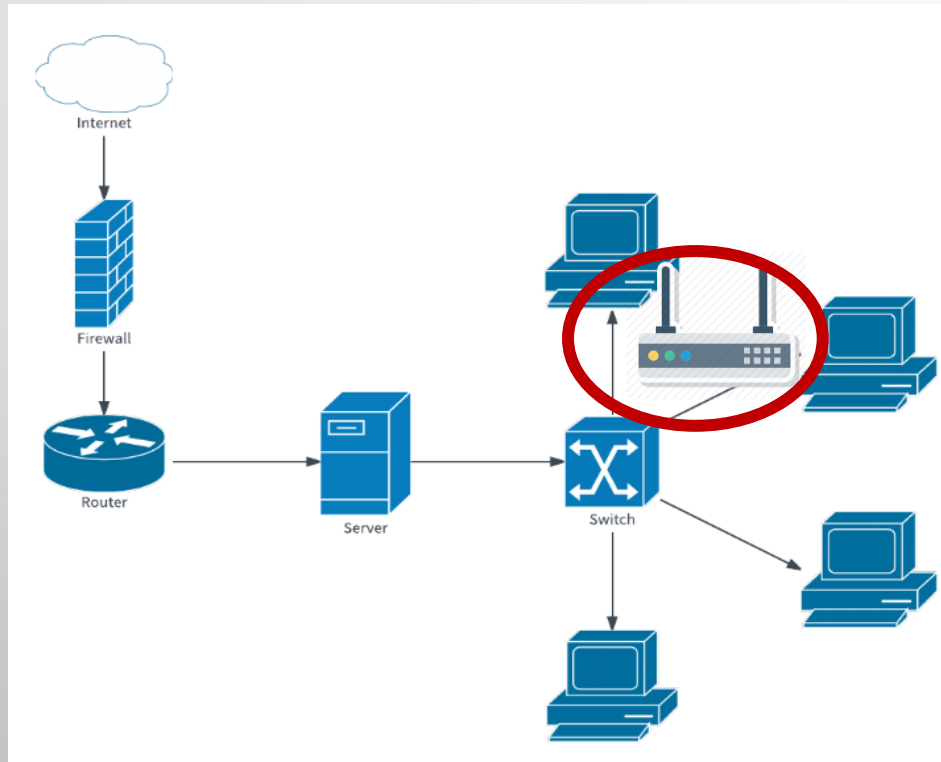
- Email
  - Office 365, default settings
- **Firewall**
  - Not properly managed
  - Open ports

# How is it Happening?



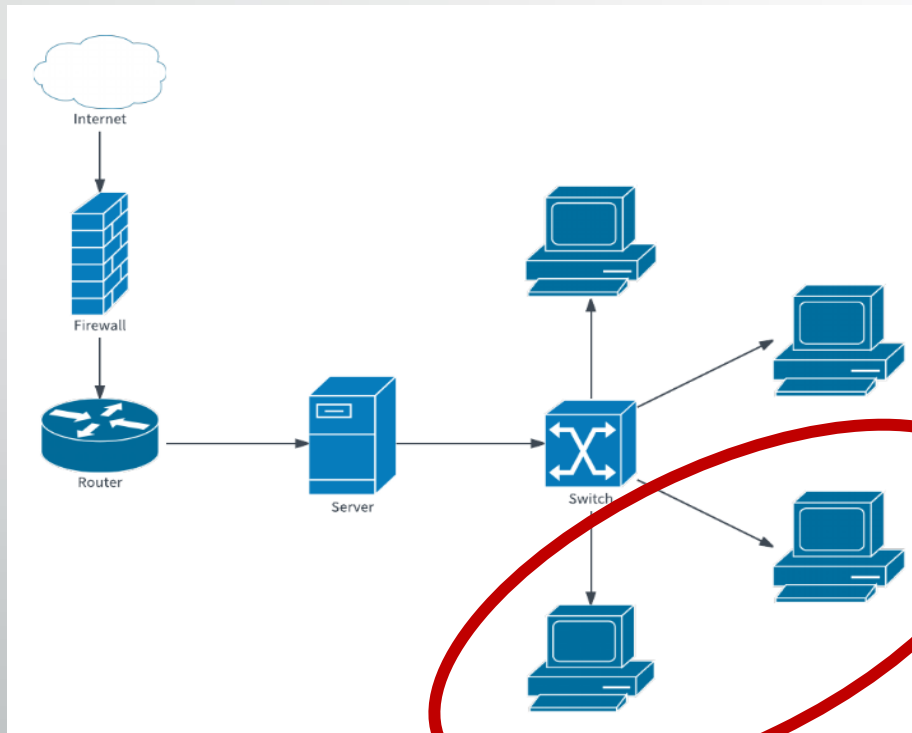
- Email
  - Office 365, default settings
- Firewall
  - Not properly managed
  - Open ports
- **RDP sessions**
- **SFTP servers**
- **Back doors**

# How is it Happening?



- Email
  - Office 365, default settings
- Firewall
  - Not properly managed
  - Open ports
- RDP sessions
- SFTP servers
- Back doors
- **Rogue wireless access point**

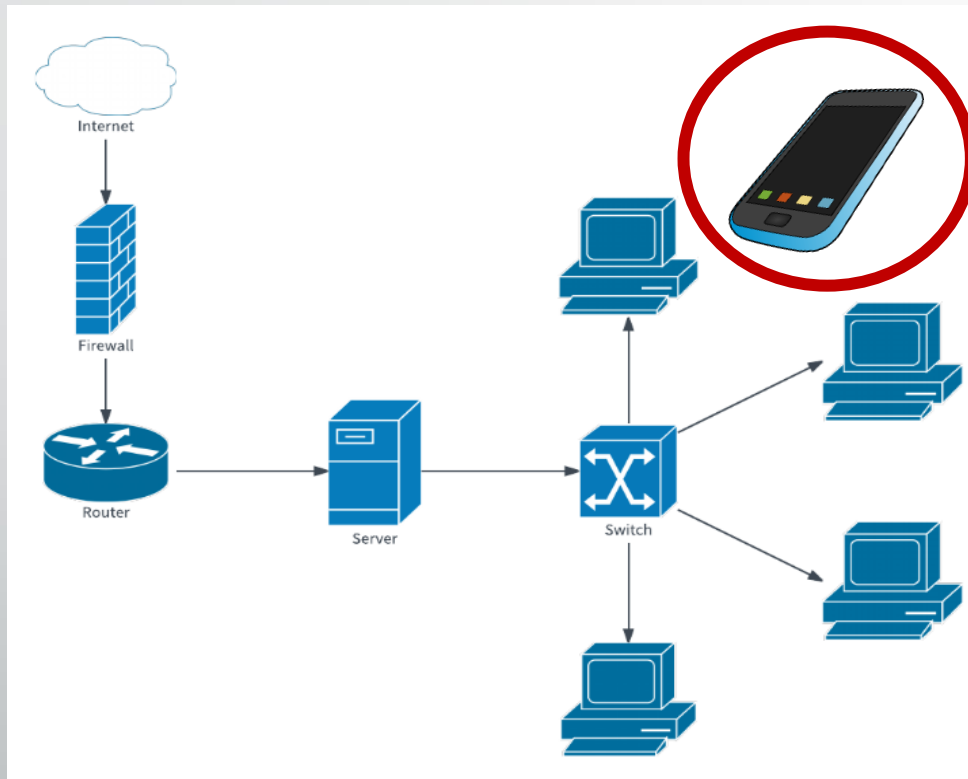
# How is it Happening?



- Email
  - Office 365, default settings
- Firewall
  - Not properly managed
  - Open ports
- RDP sessions
- SFTP servers
- Back doors
- Rogue wireless access point
- **Application vulnerabilities**
- **Old Workstations (XP)**



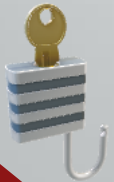
# How is it Happening?



- Email
  - Office 365, default settings
- Firewall
  - Not properly managed
  - Open ports
- RDP sessions
- SFTP servers
- Back doors
- Rogue wireless access point
- Application vulnerabilities
- Old Workstations (XP)
- **Social Engineering (ZoomInfo)**
- **BYOD**

# Once Inside

- Malware is introduced
- Programs are dropped
- Data is collected
- Backups are destroyed / encrypted
- Malware deletes itself and covers its tracks
- Encryption is launched, ransomware letter created





# Who Are They?

CrowdStrike lists 18 threat actors targeting US Healthcare providers in 2021. 14 of these originate out of Russian and Eastern Europe. The other 4 are in North Korea (Labyrinth Chollima), India (Quilted Tiger), Turkey (Percussion Spider), and Pakistan (Mythic Leopard). Top 5 in no particular order:

- Sprite Spider (Eastern Europe)
- Mythic Leopard (Pakistan)
- Velvet Chollima (N. Korea)
- Carbon Spider (Eastern Europe)
- Mallard Spider (Eastern Europe)

# COVID-Related Threats

- Exploitation of individuals looking for details on disease tracking, testing and treatment
- Impersonation of medical bodies, including the World Health Organization (WHO) and U.S. Centers for Disease Control and Prevention (CDC)
- Fake COVID vaccine registration sites (Kettering (Ohio) Health Network)
- Financial assistance and government stimulus packages
- Tailored attacks against employees working from home
- Scams offering personal protective equipment (PPE)
- Passing mention of COVID-19 within previously used phishing lure content (e.g., deliveries, invoices and purchase orders)
- HHS-OIG Fraud Alert (2.10.21)—COVID-19 Scams

# Hacking the Security Industry

- SolarWinds—up to 250 organizations impacted (2 separate attacks believed to be by Russia and China)
  - FireEye (December 2020)—nation-state attack on US and State agencies Cybersecurity Firm (FBI, NSA)
  - Microsoft
  - Malwarebytes
- Mimecast (January 2021)
- Accellion-File Transfer Appliance (FTA) vulnerabilities
  - Jones Day and Goodwin Proctor among alleged victims

# New Tactics

- Threat Tactics—bodily harm, disturbing visuals
- Releasing Data if not given money
- No longer looking for ransom to release encryption keys
- Tattlers—Release information to the web if they learn no Notice was given as required
- Rogue Privacy Activists
- Account Take-Over (ATO)—MFA is merely a “speedbump”



# Strategies & Targeting from the lips of the actors

3 Ransomware Gangs (REvil, MountLocker and LockBit) describe their strategies and target selection in recent Interviews. Notable takeaways:

- Wanted: Large Victims
- Public Naming and Shaming Works
- Cyber Insurance Pays
- RaaS Affiliates Come and Go
- Hospitals: Easy Money
- Geographical Target Selection
- No Love for (Most) Negotiators
- Reliable Payday
- 'This Crime is Scalable'
- 'Mirror to Our Neglect'



# Incident Response

Best Practices



# JOINT CYBERSECURITY ADVISORY

## Technical Approaches to Uncovering and Remediating Malicious Activity

AA20-245A

September 1, 2020



GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIARI



# “Five Eyes” Incident Response

- Joint Advisory Collaboration
  - Australia, Canada, New Zealand, United Kingdom, USA
- Cybersecurity & Infrastructure Security Agency (USA)

# “Five Eyes”: Key Takeaways

- First, collect and remove for further analysis:
  - Relevant artifacts, Logs and Data.
- Next, implement **mitigation steps** that avoid tipping off the adversary that their presence in the network has been discovered.
- Finally, consider soliciting incident response support from a **third-party IT security organization** to:
  - Provide subject matter expertise and technical support to the incident response,
  - Ensure that the actor is eradicated from the network, and
  - Avoid residual issues that could result in follow-up compromises once the incident is closed.

# COMMON MISSTEPS

Common missteps an organization can make when first responding



Mitigating the affected systems before responders can protect and recover data



Touching adversary infrastructure (Pinging, NSlookup, Browsing, etc.)



Preemptively blocking adversary infrastructure



Preemptive credential resets



Failure to preserve or collect log data that could be critical to identifying access to the compromised systems



Communicating over the same network as the incident response is being conducted (ensure all communications are held out-of-band)



Only fixing the symptoms, not the root cause



- ***Tsao v. Captiva MVP Restaurant Partners, LLC***, No. 18-14959, 2021 WL 381948 (11th Cir. Feb. 4, 2021) - threat of future harm does not create Article III **standing** unless the “hypothetical harm alleged is either ‘certainly impending’ or there is a ‘substantial risk’ of such a harm.” (Joining 2<sup>nd</sup>, 3<sup>rd</sup>, 4<sup>th</sup> and 8<sup>th</sup> Circuits)

## Litigation for Cybersecurity Breaches



# The Legal Perspective

- Common Issues in any Cyber Incident
  - Assessing a Moving Target: Data Breach Legislation
  - Coordinating Initial Response & Recovery Activities
  - Analyzing the Data
  - Determining Notification Obligations & Jurisdictions
  - Managing the Message (don't follow the Equifax or Uber examples)
  - Dealing with State & Federal Enforcement
- Pitfalls
- Best Practices

# Coordinating the Initial Response and Recovery Activities

- Informing counsel (GC and outside counsel)
- Preserving privilege and attorney work product
- Assess and determine compliance issues
- Informing Insurer (Coverage Deadlines)
- Mandatory Reporting Deadlines





# Analyzing the Data

- Be aware that there are no instant answers – this can be an iterative (and lengthy) process
- No incident is the same – analysis can take many shapes
- Know WHAT data you have
- Know WHERE data resides
  - SRA helps this process



# Cybersecurity



## Motivation

What are you going to use, a carrot or a stick?



# The **Stick** Approach to Cybersecurity

- Disruption to business operations
- Costs for mitigation/remediation
- Penalties & Fines
- CRIMINAL CULPABILITY



## The Carrot Approach to Cybersecurity

- P.L. 116-321 -Reduced penalties/fines for “Recognized Security Practices” by CEs & BAs that were in place for at least the prior 12 months
  - MITIGATE fines under SSA § 1176 (Civil Penalties) or penalties under § 1177 (Criminal Penalties)
  - result in the early, favorable termination of an HITECH audit under § 13411; and
  - MITIGATE remedies related to violations of the HIPAA Security rule
  - OCR Inquiries about “Recognized Security Practices” as part of breach investigation


## “Recognized Security Practices”

- “the standards, guidelines, best practices, methodologies, procedures, and processes developed” under the following frameworks:
  - Section 2(c)(15) of the National Institute of Standards and Technology Act (NIST Cybersecurity Framework)
  - The approaches under section 405(d) of the Cybersecurity Act of 2015 (HHS’ “*Health Industry Cybersecurity Practices: Managing threats and Protecting Patients*”)
  - Other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.
- Flexible-CE and BA determination “consistent with the HIPAA Security rule”
- No increased liability for non-compliance with “RSP”



- *Wengui v. Clark Hill, PLC, et al.*, E.D. D.C No. 19-3195 (January 12, 2021)
- *In re: Capital One Customer Data Security Breach Litigation*, E.D. Va., No. 1:19-md-02915 (June 2020)
- Cyber Attorney 1<sup>st</sup> Call—Protect AWP/ACP
- Make sure State certification/licensing law in place—PI laws required of forensic examiners
- Third-Party does NOT mean your IT vendor

## Protecting the ACP & AWP

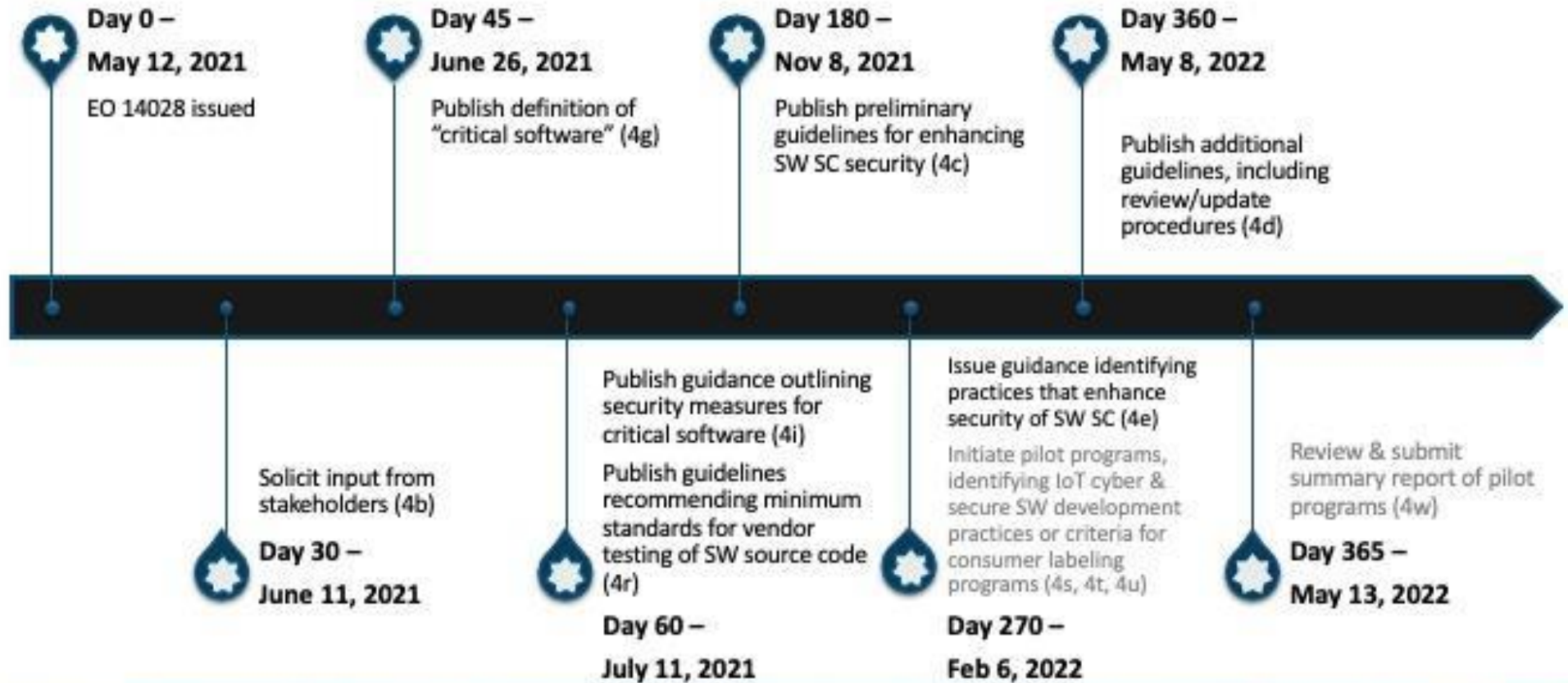


# Federal Efforts to Combat Cyber Threats

# Executive Order 14028 (May 12, 2021)

- Calls on multiple agencies, including NIST, to enhance cybersecurity through a variety of initiatives
- Section 4 directs NIST, in consultation with NSA, OMB, CISA and DNI, with input from the private sector, academia, government agencies, and others and to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security. Those guidelines are to include:
  - criteria to evaluate software security
  - criteria to evaluate the security practices of the developers and suppliers themselves
  - innovative tools or methods to demonstrate conformance with secure practices

# EO Section 4 Tasks and Timelines



# Cyber Incident Notification Act of 2021 (7.21.21)

- Bi-Partisan Bill in response to SolarWinds and Colonial Pipeline breaches, as well as Microsoft Exchange cyberespionage campaign.
- Requires all federal agencies, contractors, and organizations considered critical to U.S. national security ("Critical infrastructure) to report data breaches and security incidents to the DHS' Cybersecurity and Infrastructure Security Agency (CISA) within **24 hours** of discovery.
- "Security Incidents" requiring notification:
  - Involve or are believed to involve a nation state.
  - Involve or are believed to involve an Advanced Persistent Threat (APT) actor.
  - Involve or are believed to involve a transnational organized crime group.
  - Could harm U.S. national security interests, foreign relations, or the U.S. economy.
  - Likely to be of significant national consequence.
  - Has potential to affect CISA systems.
  - Involve ransomware

# CINA of 2012

- REPORT:
  - description of the incident
  - systems and networks affected
  - estimate of when the incident is likely to have occurred
  - information about any vulnerabilities that were exploited
  - Information about any tactics, techniques, and procedures (TTPs) known to have been used
- CISA Response to report of breach: 48 hours
- Penalty for failure to report: up to 0.5% of gross revenues from prior fiscal year and potential exclusion from federal contracting
- FOIA Exemption for Notifications
- Evidentiary Exclusion—notification cannot be used in civil or criminal cases against reporting entity, not subject to subpoena EXCEPT action of federal government (legal action) and Congress (oversight)

# OCR Resources

## HHS Office for Civil Rights in Action



### September 21, 2021 Ransomware Resources for HIPAA Regulated Entities

The HHS Office for Civil Rights (OCR) is sharing the following information to ensure that HIPAA regulated entities are aware of the resources available to assist in preventing, detecting, and mitigating breaches of unsecured protected health information caused by hacking and ransomware.

#### HHS Health Sector Cybersecurity Coordination Center Threat Briefs:

- <https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts>
  - [January 28, 2021 - ATTACK for Emotet](#)
  - [March 12, 2021 - New Ryuk Variant Analyst Note](#)
  - [April 8, 2021 - Ryuk Variants](#)
  - [May 25, 2021 - Conti Ransomware Analyst Note](#)
  - [June 3, 2021 - Ransomware Trends 2021](#)
  - [July 8, 2021 - Conti Ransomware](#)
  - [July 8, 2021 - Phobos Ransomware Analyst Note](#)
  - [August 5, 2021 - Qbot/QakBot Ransomware](#)
  - [August 6, 2021 - Lazio Ransomware Attack Analyst Note](#)
  - [August 19, 2021 - REvil Update](#)
  - [August 24, 2021 - OnePercent Group Ransomware Alert](#)
  - [August 25, 2021 - IOCs Associated with Hive Ransomware Alert](#)
  - [September 2, 2021 - Demystifying BlackMatter](#)

#### HHS Resources on Section 405(d) of the Cybersecurity Act of 2015:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients  
<https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx>
- Cybersecurity Reports and Tools <https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx>

#### OCR Guidance:

- Ransomware <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>
- Cybersecurity



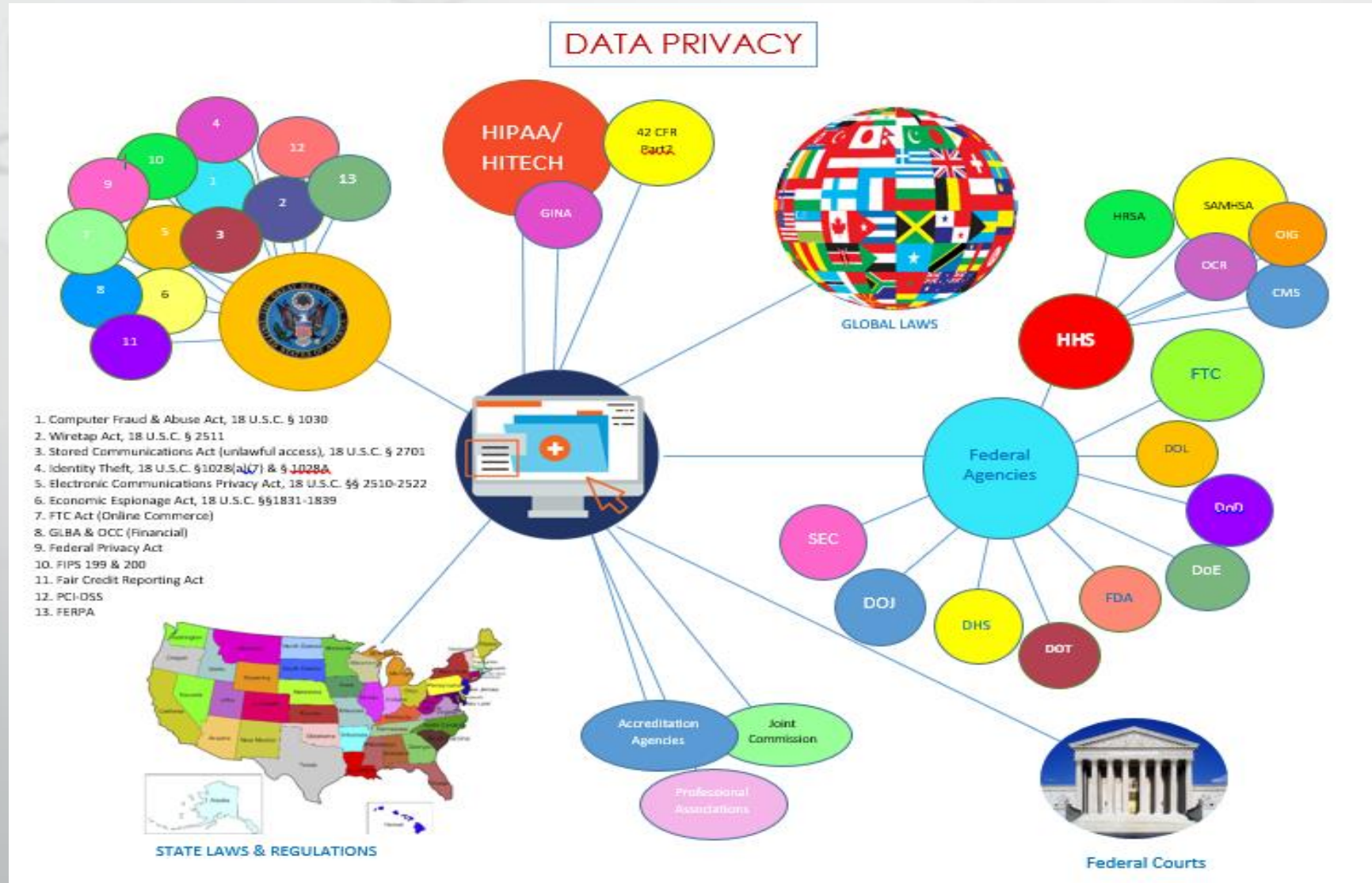
# Incident Response



# Defining the “Breach”

- First: What is a Breach/Security Incident?
  - A violation or “imminent threat of violation” of computer security policies, acceptable use policies, or standard security practices
  - Encrypted - NO BREACH!
  - Ransomware – **HHS Presumes a “Breach” if Unencrypted**
  - Risk Analysis—Low Probability? Related to Healthcare Enough to be PHI?
- Second: What was Disclosed, Published, Stolen, Accessed without Authority, Not Properly Secured...
- Do not make this determination without the assistance of counsel!

# Notification



# Notification Obligations: Understanding the Federal Landscape

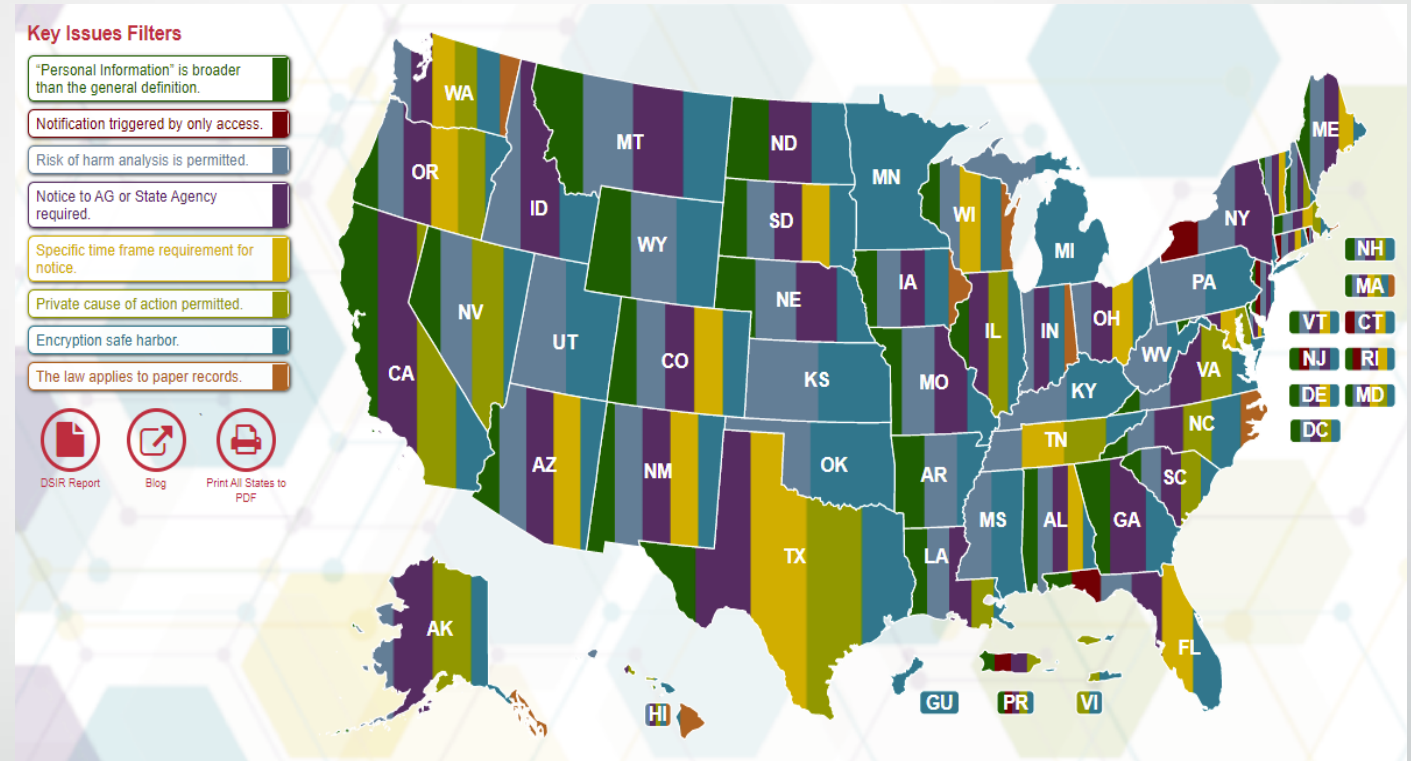
- HIPAA/HITECH & GINA (Healthcare)
- FTC Act (Online Commerce)
- GLBA & OCC (Financial)
- Federal Privacy Act (Government)
- FIPS 199 & 200
- Fair Credit Reporting Act

# Notification Obligations: Understanding the Federal Landscape (cont.)

- Computer Fraud & Abuse Act, 18 U.S.C. § 1030
- Wiretap Act, 18 U.S.C. § 2511
- Stored Communications Act (unlawful access), 18 U.S.C. § 2701
- Identity Theft, 18 U.S.C. §1028(a)(7) & § 1028A
- Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522
- Economic Espionage Act, 18 U.S.C. §§1831-1839

# Notification Obligations: Don't Forget the States

- All 50 states finally have (inconsistent) data breach laws
- Industry-Specific Legislation—
  - Insurance (NY, SC, VT)
  - Financial
  - Defense
- States may require notice to:
  - State Attorney General
  - Insurance Commissioners
  - Bureau of Consumer Affairs
  - Major Credit Bureaus (e.g., Colorado & Florida)
- And these state laws are changing rapidly...



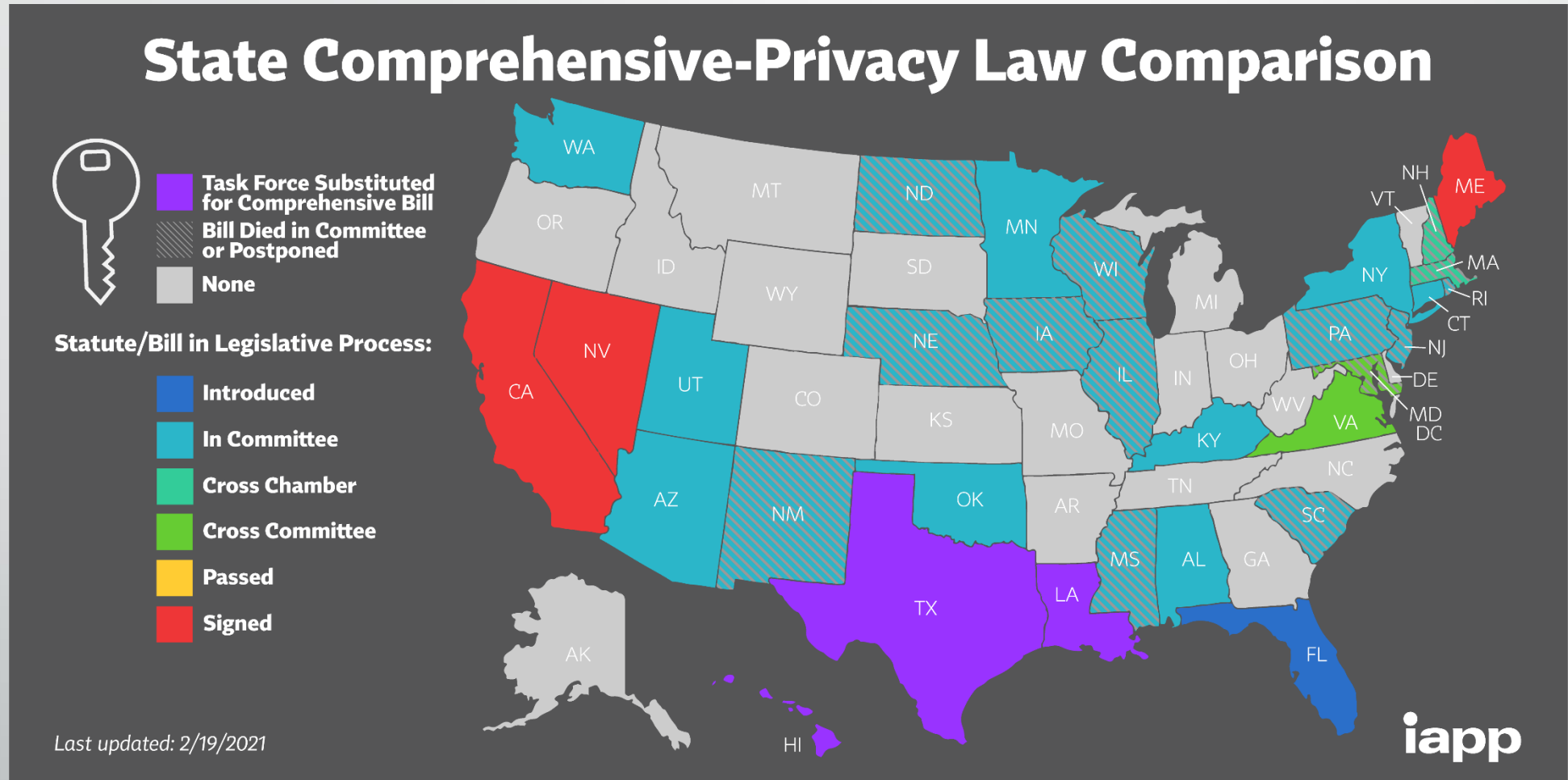
## Notification Obligations: Don't Forget the States (continued)

- In 2020, at least 280 cybersecurity bills were proposed in 38 states, Washington DC and Puerto Rico, while another 21 states, DC and Puerto Rico proposed legislation to amend existing security breach laws, although only 6 states were successful in passing the legislation. Trends in the BREACH notification laws include:
  - Establish or shorten the timeframe within which an entity must report a breach.
  - Expand definitions of "personal information" (e.g., to include biometric information, email address with password, passport number, etc.).
  - Provide an affirmative defense for entities that had reasonable security practices in place at the time of a breach.
  - Require reporting of breaches to the state attorney general.
  - Provide for free credit freezes or identity theft protection for victims of data breaches.
- Since April 2019, at least 80 bills/resolutions were introduced in 22 states and Puerto Rico. The trends in BREACH notification laws include:
  - Expanded definitions of "personal information" (e.g., to include biometric information, email address with password, passport number, etc.).
  - Set or shorten the timeframe within which a business must report a breach (w/in 72 hours of "discovery")
  - Require reporting of breaches to the state attorney general
  - Provide for free credit freezes / monitoring for victims of data breaches. (CT—24 months)

Source: National Conference of State Legislatures *Security Breach Notification Legislation/Laws*, available at: <https://www.ncsl.org/research/telecommunications-and-information-technology/overview-security-breaches.aspx> (last accessed 2.24.2021) and NCLS Cybersecurity Legislation 2020, available at: <https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx> (last accessed 3.1.21).



# 2021 Privacy Legislation



State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	Right of Access	Right of Rectification	Right of Deletion	Right of Restriction	Right of Portability	Right of Opt-Out	Right Against Automated Decision Making	Private Right of Action (s = security only)	Strict Age Opt-in for or Prohibition on Sale of Information	Notice/Transparency Requirement	Data Breach Notification	Risk Assessments	Prohibition on Discrimination (exercising right)	Purpose Limitation	Processing Limitation	Fiduciary Duty
LAWS PASSED (TO DATE)																			
California			<a href="#">CCPA</a>	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	x		x		x	x		s 16	x				x		
California "			<a href="#">Proposition 24</a>	California Privacy Rights Act (2020; effective Jan. 1, 2023)	x	x	x	x	x	x	x	s 16	x			x	x	x	
Maine <sup>v</sup>			<a href="#">LD 946</a>	An Act to Protect the Privacy of Online Consumer Information (2019; effective Jul. 1, 2020)				x		in			x				x		
Nevada			<a href="#">SB 220/Ch. 603A</a>	(2019; effective Oct. 1, 2019)					x				x	x					

# Common Obligations



# Not Just Legislatures are Enforcing PRIVACY

- Class Actions for Breaches of medical records continue:
  - November 2020—Mayo Clinic hit with 2 Class Actions based upon former employees' unauthorized access to health records of more than 1,600 patients alleging common law privacy torts and violations of the MN Health Records Act.
  - While most laws do not provide a private right of action, litigants are relying on common-law theories (negligence, privacy torts, fraud)
- CCPA Litigation
  - *Fuentes v. Sunshine Behavioral Health Group, LLC*, No. 8:20-cv-00487 (C.D. Cal. 3.20.2020)
  - *Stasi v. Inmediata Health Grp. Corp.*, No. 3:19-cv-02353 (S.D. Cal.), confirmed that the CCPA does not apply to medical information that is governed by the California Confidentiality of Medical Information Act ("CMIA") but can apply to disclosed non-medical information.
- California Privacy Protection Agency ("CalPPA")
  - created in 2020 and will take over rulemaking by July 1, 2021 and beginning January 1, 2024, the CalPPA will implement and enforce the 2020 CA Privacy Rights Act ("CPRA"), which becomes effective January 1, 2023.
- CA Attorney General continues to modify the CCPA regulations, with the 4<sup>th</sup> proposed modifications issued December 10, 2020

# Notification Obligations: Beyond the U.S.

- The EU's General Data Protection Regulations (GDPR) are considered the "gold standard" by privacy and security advocates
- MOST Countries have some type of regulation ( $\approx 111$  of 196)
- ROBUST LAWS:
  - Australia
  - Canada
  - Brazil
  - S. Korea
  - Few throughout Africa





# TIMING OF NOTICE

## The Shifting Paradigm of Notice

- 60 Days from “Discovery” (HIPAA and states following HIPAA)
- 45 Days:
  - VT (No HIPAA exemption)
  - AL, AZ, MD, NM, OH, TN, RI, WI (HIPAA exemption)
- 30 Days: Florida, Colorado, Washington
- 15 Days: CA (Medical Information under CA Health & Safety Code, § 1280.15(c))
- 90 Days: CT
- “Without unreasonable delay”: IN (no explicit number of days)

# Penalties for Delay / Insufficient Notice

- November 2019: **Sentara Hospitals** settles potential HIPAA Breach Notice violation for \$2.175 million and CAP for notifying only 8 of 577 individuals whose PHI was mismailed, despite OCR's explicit directive to notify all 577
- May 2019: **Touchstone Medical Imaging** was fined \$3,000,000 for failure to timely investigate and notify of a Breach.
- March 2019: **UCLA** Class action Settlement. Plaintiffs claimed UCLA failed to timely notify them of breach that occurred in October 2014, but only notified them in May 2015 when it was actually discovered PHI was impacted
- June 2017: **CoPilot Provider Support Services, Inc.** settled NY AG action for \$130,000 due to untimely notification to patients of breach (over 1 year)
- January 2017—**Presence Health** settles alleged untimely breach notification claim for \$475,000 and CAP
  - Paper-based PHI of 836 patients lost



# Paying the Cybercriminals

## A Catch-22

# The PROs

- Victims get their information back to continue operations
- Avoidance of public humiliation (and public perception) occasioned by a “leak” of data by the threat actor when ransom is not paid



# The CONs

- FBI: Advises against paying, but recognizes the need to do so
- FinCEN—October 2020 Advisory—Reminder of financial institutions obligation to report “Suspicious Unlawful Activity”
- OFAC Sanctions



# OFAC Advisory

## Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

[October 2020 & **UPDATED 9.21.21**]

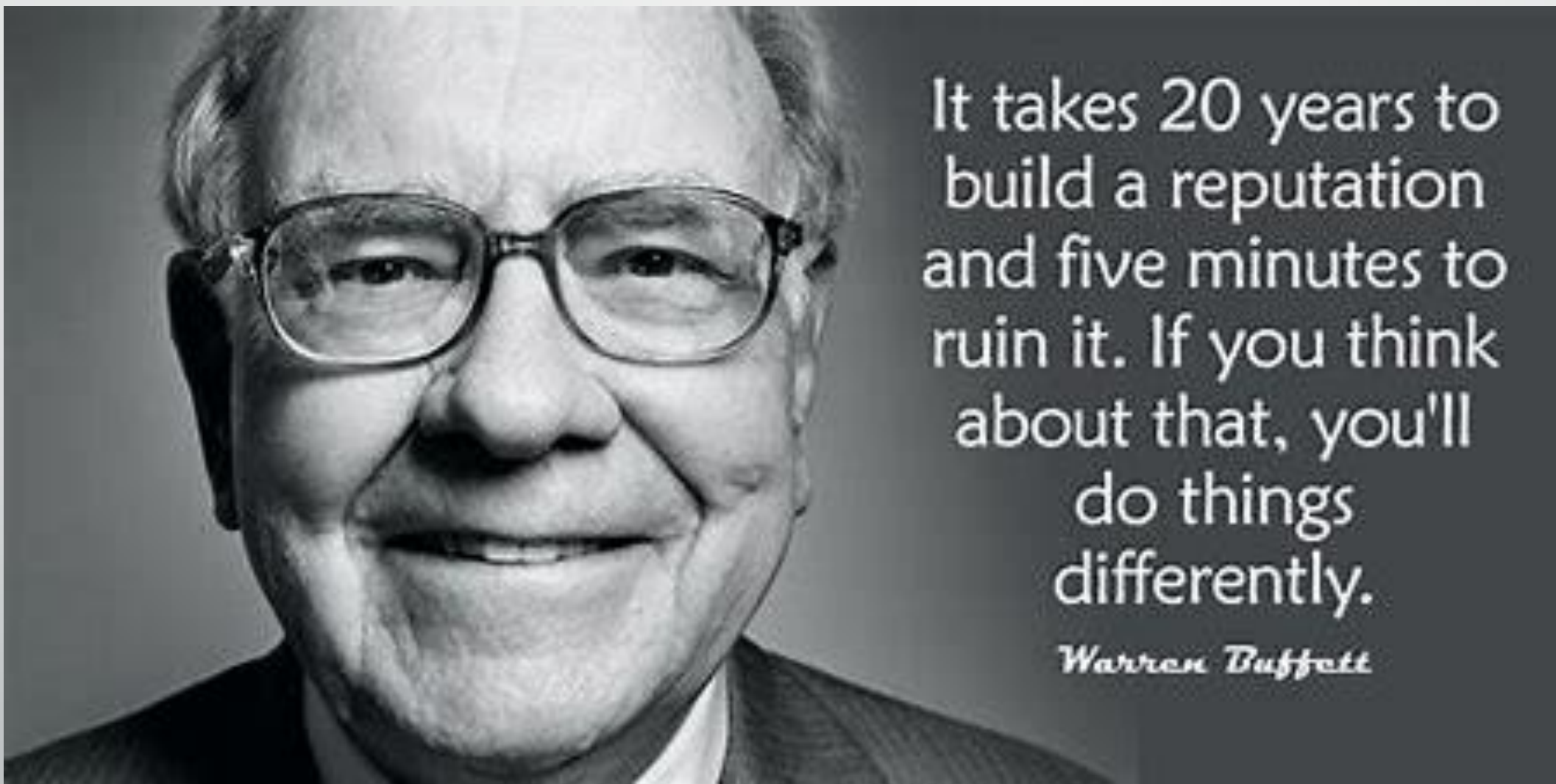
- Outlines potential sanctions to **victims** of ransomware for engaging in a transaction with prohibited individuals and entities (SDN List).
- OFAC Designated Actors:
  - Evgeniy (Cryptolocker developer)
  - Lazarus Group (NK), Bluenoroff & Andariel (WannaCry 2.0)
  - Evil Corp/Maksim Yakubets (Russian Dridex developer)
  - SUEX OTC, S.R.O (virtual currency exchange- 40% of KNOWN transactions with illicit actors)
- “Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations”
  - “OFAC may impose civil penalties for sanctions violations based on **strict liability**, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.”
  - OFAC Authority: International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA)

# Investigation



## Dealing with Federal & State Enforcement Authorities

- Establish a timeline of events
  - Security Incident “Discovery”
  - Forensic Examination Process, Issues, etc.
  - Notice (agency, individuals, media, substitute...)
  - Risk Analysis (HIPAA Breach Response, State requirements)
    - Sentara Hospital—Misconstrued reporting obligation = \$2.175M
- Preparing documentation supporting compliance
- Responding to investigatory demands and subpoenas
- Meetings and negotiations with government agencies
- Be prepared to demonstrate implementation of “recognized security practices” (mitigation)



# Safeguards & Best Practices



# Safeguards (What can I do now?)

- **Multi-Factor Authentication Everywhere**
- Third-party Internal & External Vulnerability Audit
- Cloud based system audits (Office 365 etc.)
  - Microsoft Score may not be enough
- Make the changes suggested
- Consider layered security
  - SIEM-SOC
- Blue, Red, Purple Team & Tabletop Exercises
- On-going education and testing of workforce
- Enforce policies and procedures
- SOC-Cyber Certification





# What Does “All Safe” Really Mean?



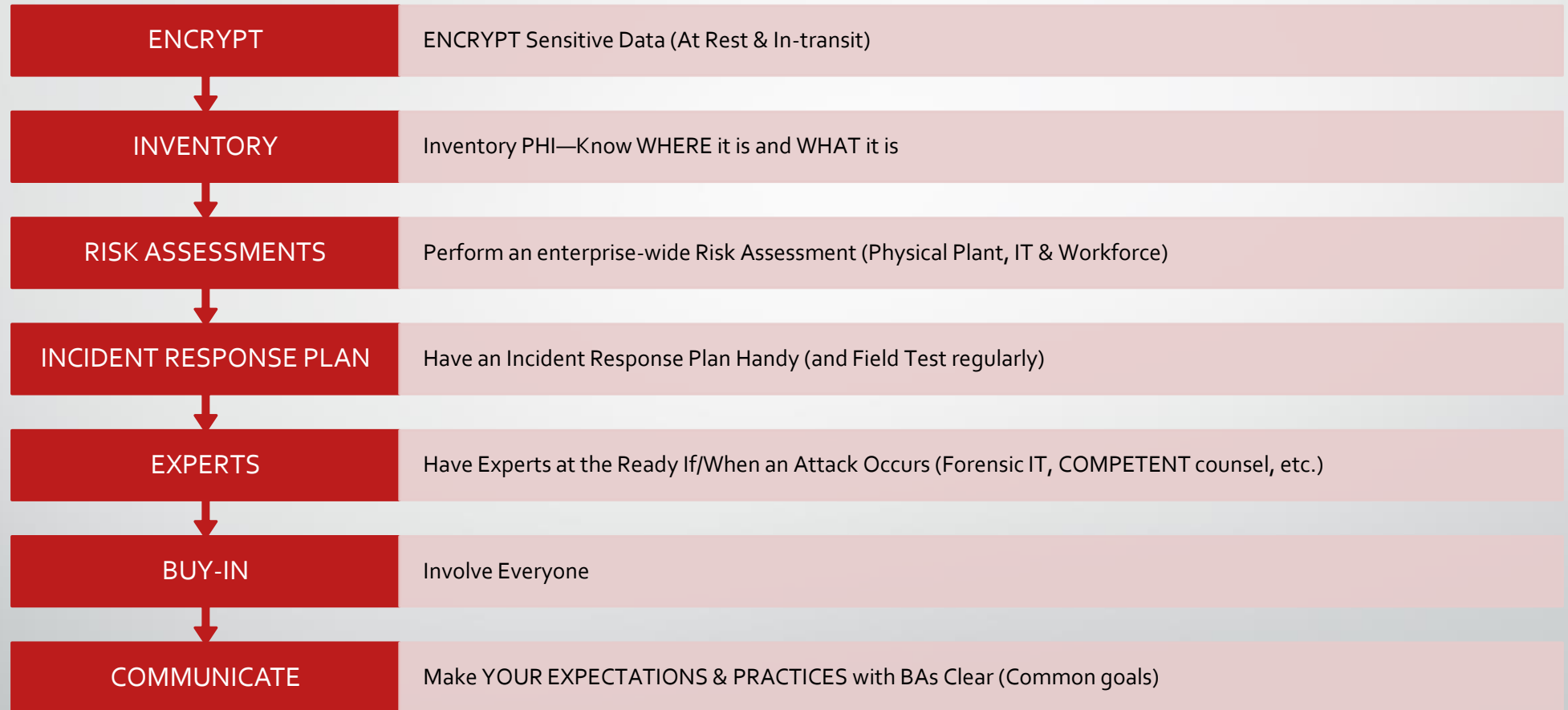
## #1 phrase heard from CEO's

“My IT Department tells me we are completely safe.”

## #2 phrase heard from CEO's

“Yes, we are safe because we are SOC compliant.”

# Best Practices Overall





## Best Practices Overall (cont.)

- Implement Robust Password Policy (DUAL-FACTOR, VPN, etc.)
- Robust TRAINING of ENTIRE workforce (Annual)
- Conduct Table-Top Drills
- Segregate & Secure High Risk Information, Operations & Workers (back-up information)
- Incorporate Security By Design
- Enable Network Security Monitoring & Review of Log Files
- DOCUMENT, DOCUMENT, DOCUMENT!

# Best Practices: Cyber Liability Insurance

- \$1-2M coverage *minimum*
- Coverage Basics:
  - **1<sup>st</sup> Party Costs:** Notification, Forensics, Legal Assistance, Credit Monitoring, PR Firms
  - **3<sup>rd</sup> Party Coverages:** Defense Costs & Settlements
  - **Network Security:** Loss or Damage to a Network & Data, 1<sup>st</sup> & 3<sup>rd</sup> Party Costs (may include lost income—business interruption)
  - **Media Liability:** Web Content (Defamation: Libel & Slander)
  - **Fines & Penalties** (HIPAA, PCI)
  - **eVandalism; Extortion; Ransom**
  - **Property Loss** from Cyber Perils (Internet of Things)
- Research / Review Options (and claims history) before you buy
- **POSSIBLE Coverage under Commercial Crime policy?** [G&G Oil Co. of Ind., Inc. v. Continental W. Ins. Co., 2021 WL 1034982 \(Ind. Mar. 18, 2021\).](#)

## Best Practices on the IT Side

- Eliminate Unnecessary Data (and USERS)
- Conduct Ongoing & Active Risk Analysis
- Collect, Analyze & Share Incident Data
- Collect & Share Tactical Threat Intelligence (ISAC/ISAO)
- Focus on Better & Faster Detection
- Geolocation Blocking (eliminate non-customer countries)
- Backups (Third-Party or SaaS-based backups)
- Password Policy
  - Auto expiring
  - Two-factor authentication
  - Pass-PHRASE

# Best Practices on the IT Side (cont.)

1

## Access

- Access Control Levels (Admin, Dept., Staff...)

2

## Track

- Track Workforce: Who's Who, What they Do & When they Go

3

## Establish

- Establish Metrics: "Number of Compromised Systems" & "Mean Time To Detection" in Networks; Use Metrics to Drive Security

4

## Evaluate

- Evaluate Threat Landscape to Prioritize Treatment Strategy (It's not a "One-Size Fits All" World)

# Best Practice: Managing the Message



Engage a PR team



Have a form script at  
the ready



Get your facts  
straight before you  
release the message



Ensure all required  
aspects are in the  
message

## Best Practices: Communications

Be	Be open and sincere. Admit fault if it is yours and accept responsibility.
Provide	Provide details. Explain why the situation took place.
Mitigate	Mitigate. Make conclusions out of the disaster and describe solutions for affected users.
Educate	Educate. Explain how to prevent similar issues in the future.
Invite	Invite discussion.
Involve	Involve stakeholders.

# Questions

**Debra A. Geroux, JD, CHC, CHPC**  
Shareholder  
Butzel Long, a professional corporation  
[geroux@butzel.com](mailto:geroux@butzel.com)  
248.258.2603

**Scott Wrobel**  
Co-Owner, N1 Discovery  
[scott.wrobel@n1discovery.com](mailto:scott.wrobel@n1discovery.com)  
248-498-4131