





*Cybersecurity & Incident Response: The Nuts and Bolts  
of Avoiding & Responding to a Security Incident*  
HCCA's 24th Annual Compliance Institute  
March 29, 2020



1

## **INTRODUCTIONS**

- Debra A. Geroux, JD, CHC, CHPC, Shareholder, Butzel Long
- Scott Wrobel, Co-Owner, N1 Discovery

2

2

## Overview

- Cyber Risks in Healthcare
- Incidents Response: The Legal and Logistical Perspectives
- Lessons Learned
- Best Practices



## Cyber Risks

Presented by: Scott Wrobel

## Agenda

- New Cyber Facts
- Changes in Cyber Attacks
- The Impact & Cost
- Why is it Happening
- How is it Happening

5

5

## 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%

6

6

# Changes in Cyber Attacks

## Well-funded, Smarter, Advanced, Patient

- Increased \$\$\$ in ransomware
- Educated, trained and experienced
- Sophisticated malware
- Thorough, diligent, patient

# Ransom(ware) By the Numbers-

IBM Security 2019 Cost of a Data Breach Report\*

Global Averages		United States Averages	
Average total cost of a data breach		Average total cost of a data breach	
\$3.92M		\$8.19M	
Average size of a data breach	25,575 records	Average size of a data breach	25,575 records
Cost per lost record	Time to identify and contain a breach	Cost per lost record	Time to identify and contain a breach
\$150	279 days	\$242	245 days
Highest country average cost of \$8.19 million	Highest industry average cost of \$6.45 million	Country rank for total cost	Highest industry average for cost per record
United States	Healthcare	1	Healthcare

### Activity-Based Costs

- Investigations and forensics (root cause)
- Identifying probable victims
- Organizing an incident response team
- Communication and PR outreach
- Notification and other required disclosures to victims and regulators
- Call Center readiness
- Audit and consulting services
- Legal services (defense & compliance)
- Free or discounted services to victims
- Identity protection services
- Reputational Damages / Lost business
- Customer acquisition and loyalty program costs

\*Available at: [https://www.ibm.com/downloads/cas/2021/07/08\\_2424288004845456118\\_1580746139-91450366.1580746139](https://www.ibm.com/downloads/cas/2021/07/08_2424288004845456118_1580746139-91450366.1580746139) (last accessed February 3, 2020).

## A Look at the Numbers

- Over 2 billion in ransomware revenue (2018)
- 850 million ransomware infections (2018)
- CryptoWall alone generated \$320M revenue
- City of Atlanta \$17M+ to rebuild environment
- NOLA \$7M+ (only \$3M covered by insurance)
- 1.5M new phishing sites are created every month
- A victim of ransomware will occur every 14 seconds (2019)

Sources: Webroot, Cyber Security Ventures, Symantec, SC Magazine

9

9

## U.S. Healthcare Industry (Source: 2019 IBM CDBR)

- Average Total Cost of Data Breach: \$6.45M
- Average Cost per Record: \$429
- Root Causes: Malicious Attacks (51%), System Glitch (25%); Human Error (24%)
- Healthcare Customer Turnover nearly DOUBLE the average (7% v 3.9%)
- Lifecycle of Data Breach: 329 (average is 279) to identify and contain
- Delivery Method (Generally): Email (94%) and Web (23%)
- Threat Actors: Internal (59%) & External (42%) top list

10

10

# Who Are They?

## Top Hacking Groups / Threat Actors

- Grim Spider (Russia)
- Lazarus Group (North Korea)
- Sofacy aka Fancy Bear (Russia)
- MuddyWater (Iran)
- APT 15, Stone Panda (China)
- Anonymous (Global)
- The Shadow Brokers (Unknown, poss. Russia)
  - Stole NSA secrets

11

11

# 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)
- **Human error**

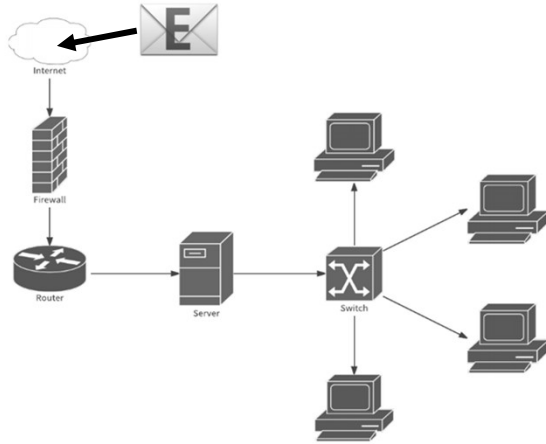


12

12

# How is it Happening?

- **Email**
  - Office 365, default settings

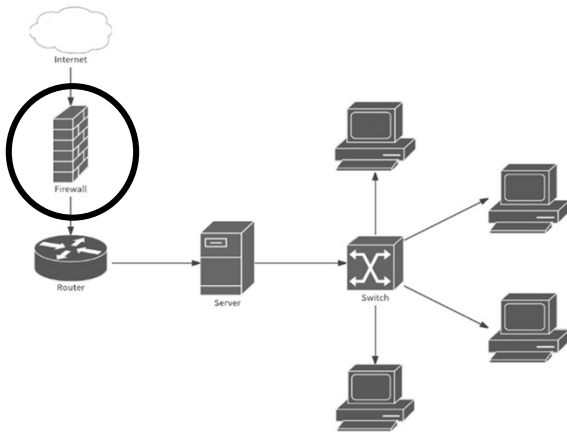


13

13

# How is it Happening?

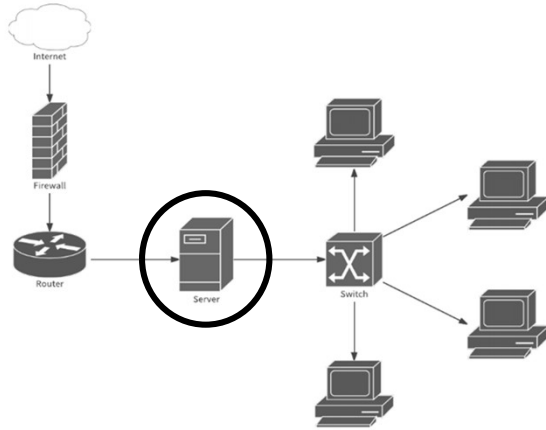
- **Email**
  - Office 365, default settings
- **Firewall**
  - Not properly managed
  - Open ports



14

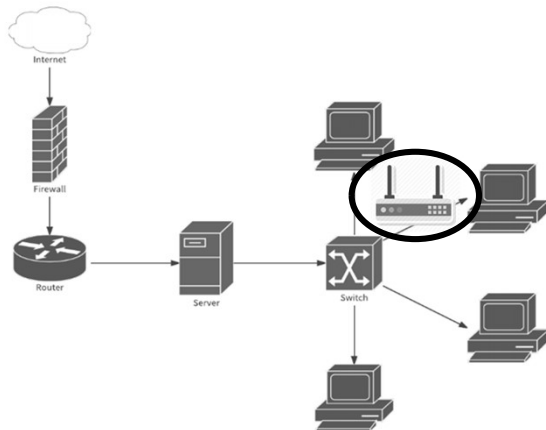
14

# How is it Happening?



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

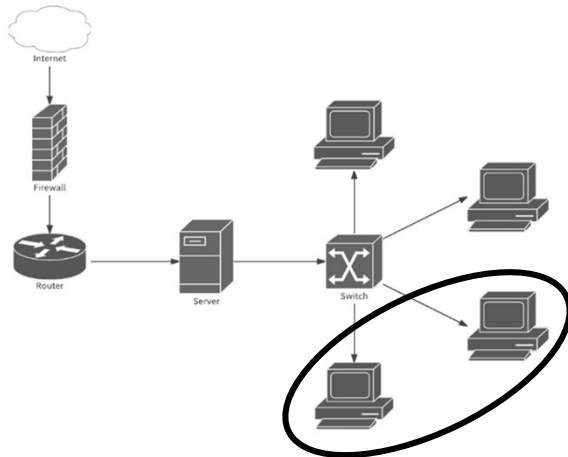
# How is it Happening?



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

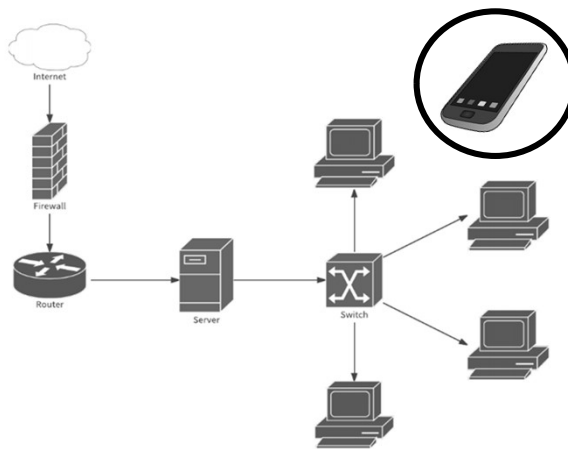


# How is it Happening?



- 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**
- **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

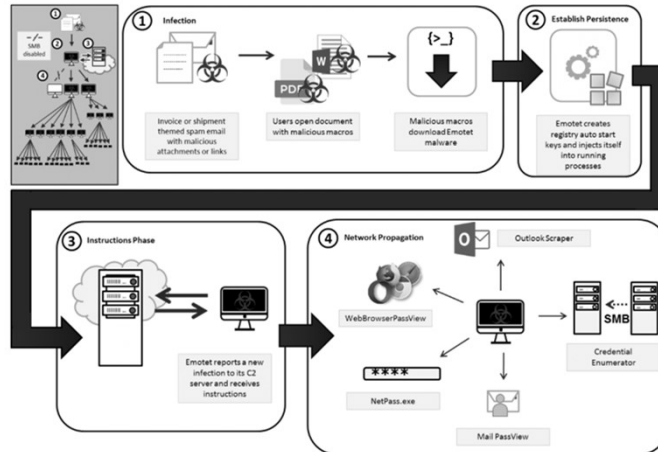


# Current THREATS

## Threat 1: Emotet Malware

Source: CISA Alert (TA18-201A)

- Disseminated through malspam (emails containing malicious attachments or links) using familiar branding (*i.e.*, paypal)
- **COSTLY REMEDIATION:** up to \$1 million per incident to remediate (government); Private sector remediation likely greater



21

21

## Threat 2: Ryuk

- Ryuk is a crypto-ransomware that uses encryption to block access to systems/devices or files until the ransom is paid
- It is a tailored attack spread as a secondary payload through other malware, most notably TrickBot and Emotet, as well as through RDS
- FBI reports 100+ businesses in US and globally have been targeted since August 2018 (*Source: FBI Flash May 2, 2019*)
- More than 500 schools hit in 2019 (*Source: Zdnet.com*)
- December 2019: NOLA declares State of Emergency due to suspicious activity linked to Ryuk
- November 2019: 2 EMR vendors (Virtual Care Provider Inc. and Casamba) locked out of EMR impacting nursing homes and post-acute providers and clinics throughout US
- October 2019: DCH Regional Medical Center, Northport Medical Center and Fayette Medical Center in Alabama locked out of EHR, forcing systems to suspend scheduled testing and procedures

22

22

## Threat 3: "Other" Ransomware

- Steal files before encryption
- Threaten victim with publicly exposing files if ransom denied
  - December 2019: Pensacola, FL (Maze)-2GB released to show impact
    - Hackers did not impact "socially significant services (hospitals, 911, etc.)" (Source: [CISO MAG\\_12/27/19](#))
  - January 2020: Medical Diagnostic Laboratories (MDLab) information leaked due to failure to pay ransom (Source: [HIPAA Journal](#))
  - January 2020: Enloe Medical Center's network encrypted by unknown malware, including EMR and phones (Source: [HIPAA Journal](#))

23

23



## Ransom(ware) By the Numbers (cont.)

- Q4 of 2019: Average ransom payment \$84,116 (up 104% from Q3 of 2019)
- Ryuk and Sodinokibi have moved into the large enterprise space and are focusing their attacks on large companies where they can attempt to extort the organization for a seven-figure payout.
- Ryuk ransom payments reached a new high of \$780,000 for impacted enterprises.
- Smaller ransomware-as-a-service variants such as Dharma, Snatch, and Netwalker continue to blanket the small business space with a high number of attacks, but with demands as low as \$1,500.

Source: Coware Q4 Marketplace Ransomware report: <https://www.coware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate> (accessed January 31, 2020).

24

24

## Safeguards (What can I do?)

- Third-party Internal & External Vulnerability Audit
- Cloud based system audits (Office 365 etc.)
- Make the changes suggested ↑
- Consider layered security
  - SIEM-SOC
- On-going education and testing of workforce
- Enforce policies and procedures
- SOC-Cyber Certification



25

25

## 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.”

26

26

# Your Network: Is a Page Missing?



27

27

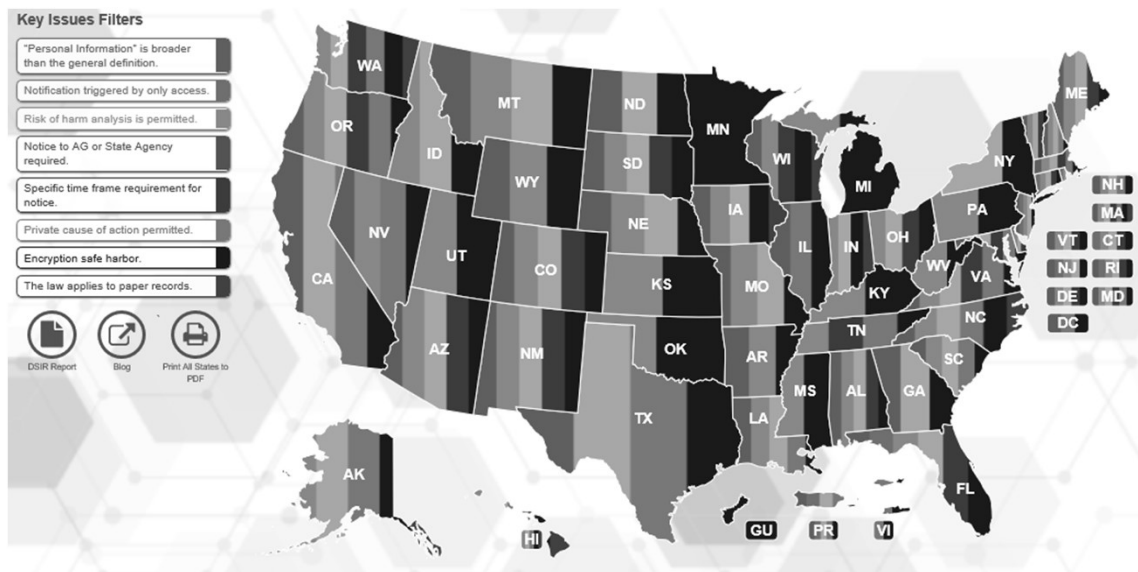


28

28

# 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



 BUTZEL LONG

31

31

## 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



 BUTZEL LONG

32

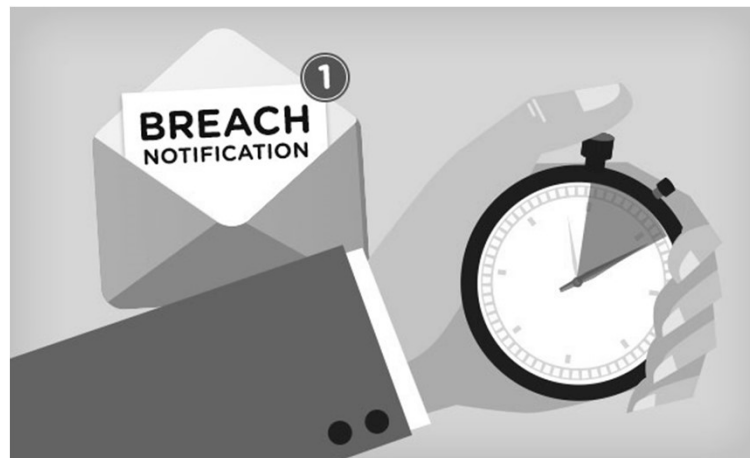
32



## Defining the “Breach”

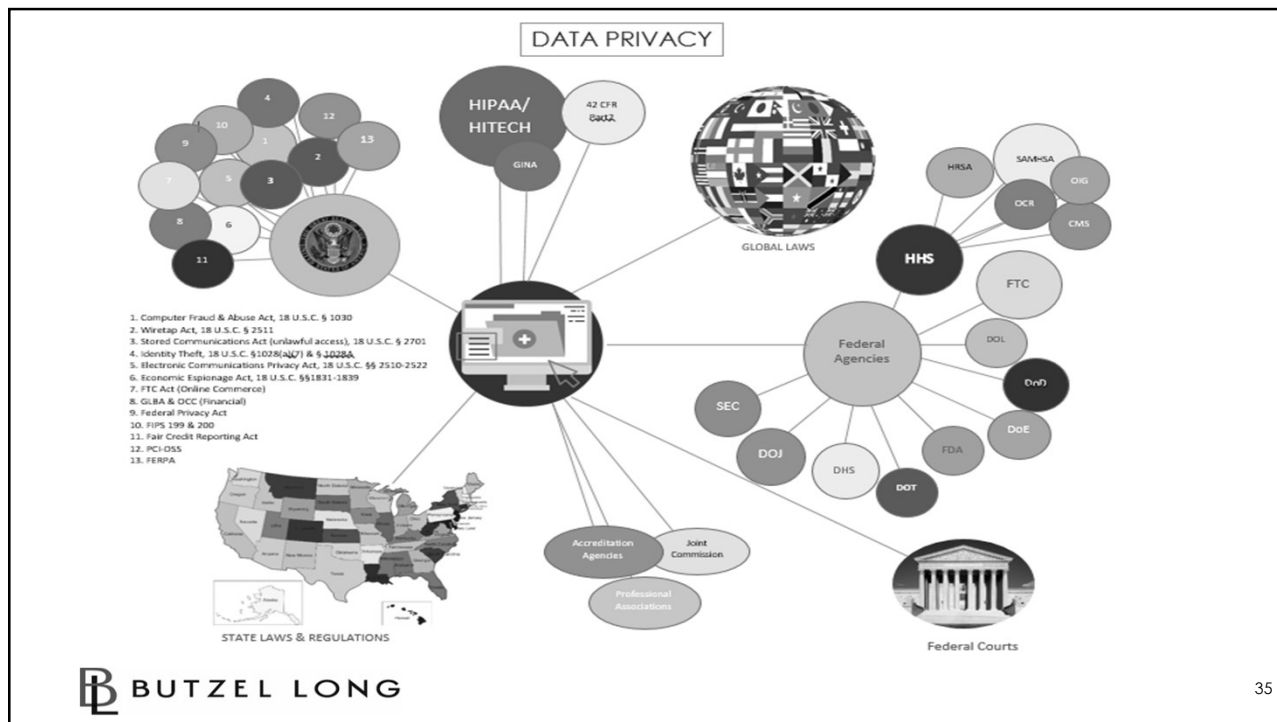
- **First: What is a Breach/Security Incident?**
  - A violation or “imminent threat of violation” of computer security policies, acceptable use policies, or standard security practices
  - Encrypted - NO BREACH!
  - Ransomware – **HHS Presumes a “Breach” if Unencrypted**
  - Risk Analysis—Low Probability? 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!**

33



**NOTIFICATION**

34



35

## 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

**BUTZEL LONG**

36

36

## 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



37

37

## 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...



38

38

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

- In 2018, there were 265 **new** cybersecurity and data privacy bills proposed in 35 states. Key legislation included:
  - Ohio Data Protection Act (2018 SB 220)
  - California Consumer Privacy Act (often compared to the EU's General Data Protection Regulations – GDPR)
- Since April 2019, more than 160 bills/resolutions have been introduced in 36 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)



State	2019 Passed Privacy Laws	Updates to Data Breach Notification Statutes	Passed Industry Specific Data Breach Notification Laws	2019 States to Watch – Privacy Laws	2020 Proposed Legislation
Alabama					
Arkansas					
California					
Connecticut					
Delaware					
Florida					
Hawaii					
Illinois					
Maine					
Maryland					
Massachusetts					
Michigan					
Mississippi					
Nebraska					
Nevada					
New Hampshire					
New Jersey					
New York					
Ohio					
Oregon					
Pennsylvania					
Rhode Island					
South Carolina					
Texas					
Virginia					
Washington					

Source: Butzel Long Counsel's Corner (February 4, 2020), available at [www.butzel.com](http://www.butzel.com).



## Not Just Legislatures are Enforcing PRIVACY

- PA Supreme Court: Companies must protect employee's data
- State Attorneys General are making significant strides to require notice
- Private Plaintiffs (standing?) are suing individually and through class actions
  - CVS/Caremark--\$4.35M (November 2019) Settlement for mishandled HIV mailing for 6,000
  - Experian--\$74M (June 2019)--\$32M to victims; \$42M to overhaul its IS program
  - Premera--\$32M (2019)
  - UCLA--\$7.5M (March 2019) Settlement for Failing to timely notify 4.5M of breach (OCR found response satisfactory)
  - Marriott, Exactis & Equifax—Class Actions filed within DAYS of announcement (2018)
  - Yahoo—Filed within months of announcement (2016)
  - Anthem--\$115M Settlement (June 2017)

## 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 (eff 3/1/20)
- 90 Days: CT

## Penalties for Delay / Insufficient Notice

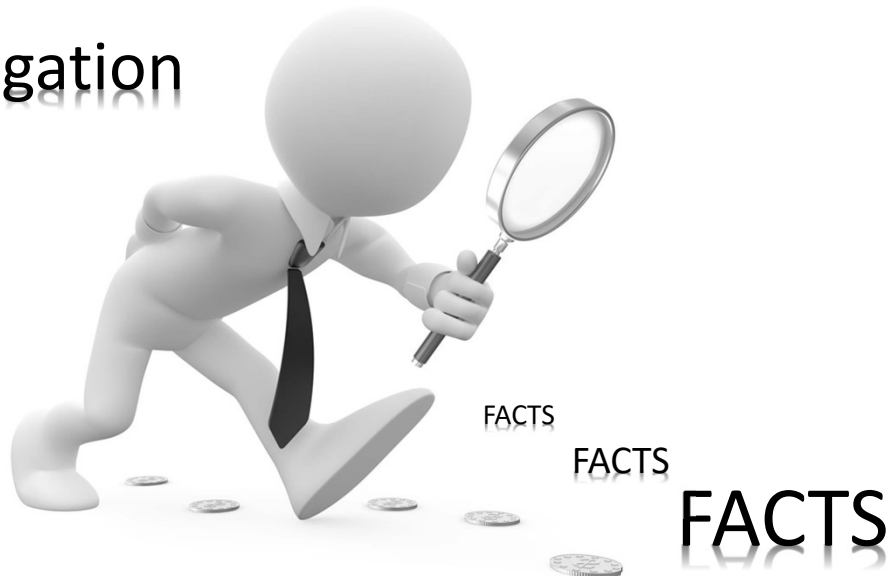
- November 2019: **Sentara Hospitals** settles potential HIPAA Breach Notice violation for \$2.175 million and CAP for notifying only 8 of 577 individuals whose PHI was mismailed, despite OCR's explicit directive to notify all 577
- March 2019: **UCLA** Class action Settlement. Plaintiffs claimed UCLA 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
- January 2017—**Presence Health** settles alleged untimely breach notification claim for \$475,000 and CAP
  - Paper-based PHI of 836 patients lost



45

45

## Investigation

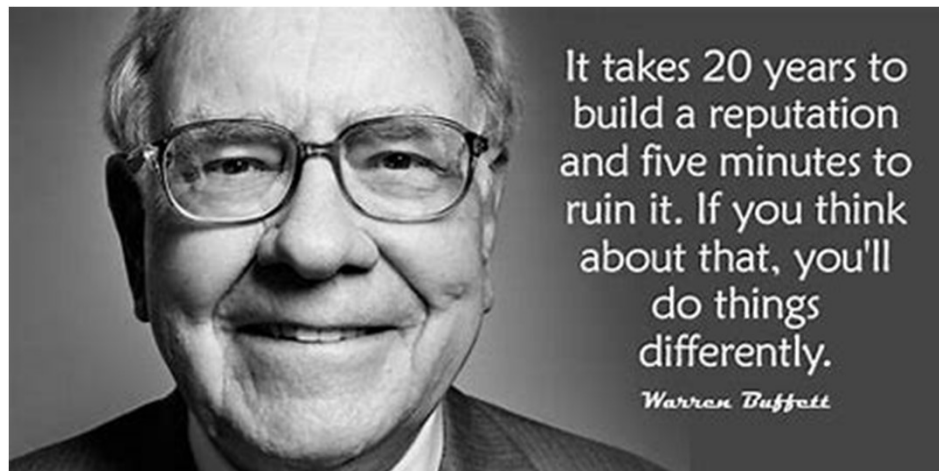


46

46

## 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





## Managing the Message: Equifax

- On September 7, 2017, Equifax revealed that months-long improper access led to the breach of personal identifying information of over 143 million people. The company waited and, after six weeks, decided to disclose the breach.
- The CEO (Richard Smith) testified in front of Congress and blamed a single employee who failed to update software on one server.
- Shortly after, Smith resigned, retaining over \$90,000,000 in compensation that he would have lost if fired.
- 2019 FTC Settlement at least \$575 Million (possibly \$700M)

## Managing the Message: Uber

- The narrative, according to NPR: “Uber Pays \$148 Million Over Yearlong Cover-Up Of Data Breach”
- In 2016, Uber discovered the incident and, under the leadership of its former CEO, paid hackers \$100,000 as a “bug bounty”
- Later, in November 2017, Uber’s NEW CEO revealed that the hackers had downloaded the names, email addresses and mobile phone numbers of over 57 million users around the globe
- Moral: Ignoring or not fully appreciating the extent of a cybersecurity incident can have devastating financial and reputational impact

# Best Practice

- ①
- ②
- ③



## Best Practices Overall

- ENCRYPT Sensitive Data (At Rest & In-transit)
- Inventory PHI—Know WHERE it is and WHAT it is
- Perform an enterprise-wide Risk Assessment (Physical Plant, IT & Workforce)
- Have an Incident Response Plan Handy (and Field Test *regularly*)
- Have Experts at the Ready If/When an Attack Occurs (Forensic IT, COMPETENT counsel, etc.)
- Involve Everyone
- Make YOUR EXPECTATIONS & PRACTICES with BAs Clear (Common goals)

## 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

## Best Practices on the IT Side

- Eliminate Unnecessary Data
- 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.)

- Access Control Levels (Admin, Dept., Staff...)
- Track Workforce: Who's Who, What they Do & When they Go
- Establish Metrics: "Number of Compromised Systems" & "Mean Time To Detection" in Networks; Use Metrics to Drive Security
- 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 open and sincere. Admit fault if it is yours and accept responsibility.
- Provide details. Explain why the situation took place.
- Mitigate. Make conclusions out of the disaster and describe solutions for affected users.
- Educate. Explain how to prevent similar issues in the future.
- Invite discussion.
- Involve stakeholders.

# About Butzel Long

Cybersecurity & Privacy Specialty Team

[www.butzel.com](http://www.butzel.com)

A LexMundi Member



A LEADING LAW FIRM WITH OFFICES IN MICHIGAN, NEW YORK CITY, WASHINGTON D.C., AND CHINA.

Founded in 1854, Butzel Long has played a prominent role in the development and growth of several major industries. Business leaders have turned to us for innovative, highly-effective legal counsel for over 165 years. We have a long and successful history of developing new capabilities and deepening our expertise for our clients' benefit. We strive to be on the cutting edge of technology, manufacturing, e-commerce, biotechnology, intellectual property, and cross-border operations and transactions.



59

59



## About N1D

- Digital Forensics
- eDiscovery
- Cybersecurity
- Intelligence Services

60

60



**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

61