

Ransomware

WannaCry Attack — Threat or Fake News?:

- ❖ A ransomware attack that impacted more than 300,000 people across 150 countries in less than two days.
- ❖ - Stroz Friedberg, 2018 Cybersecurity Predictions, at p. 18 (2018)

How it Happens:

- ❖ Hackers gain access to your computer's file system by installing a program via phishing link/attachment or by poorly configured Remote Desktop Protocol service.
- ❖ The ransomware prevents a user from accessing the operating system, or encrypts all the data stored on the computer.
- ❖ The user asks the ransom to pay a fixed amount of money, as opposed to decrypting files or allowing access again to the operating system.

Best Practices:


- ✓ Maintain a robust, off-site backup of data
- ✓ Properly configure Remote Desktop Protocol services.

\$5B

Is the estimated global cost for organizations of ransomware attacks in 2017 — up 400% from 2016.


Stroz Friedberg (2018), 2018 Cybersecurity Predictions, at p. 19 (2018)

Source: BakerHostetler, 2018 Data Security Incident Response Report, at p. 4 (2018).



Compromise

s CEO, asking human
loyee W-2 information:

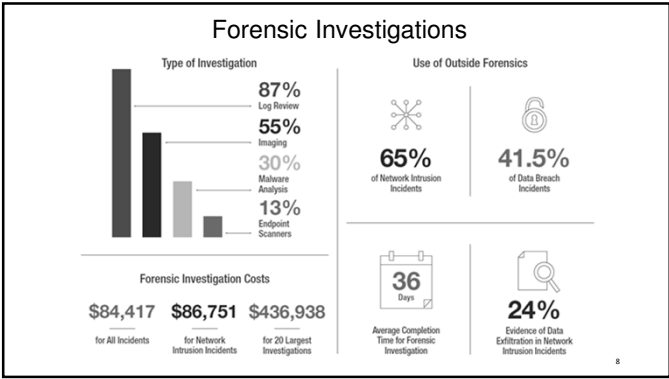


as wage
...pe, you
can send it as an attachment. Kindly prepare the lists and email
them to me asap.

New Area Prone to Attack:

- In 2017, hackers phished online payroll management account credentials used by corporate HR professionals.

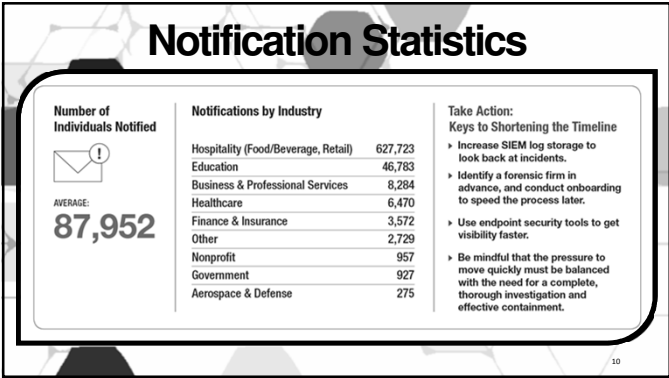
7

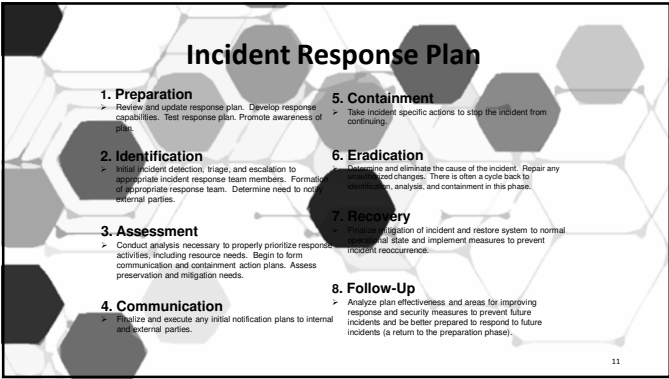


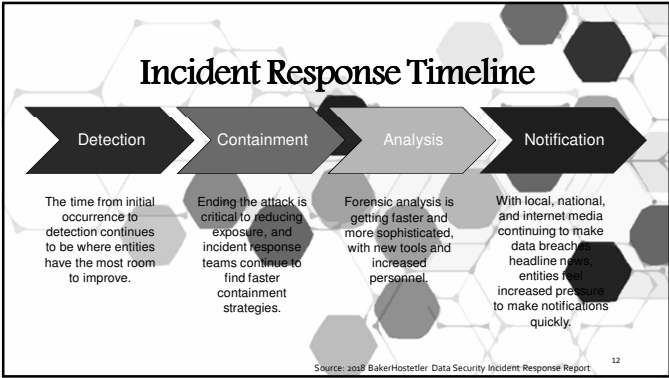
Incident Response and Notification Process



9







Let Forensics Drive the Decision Making

- ❖ Know where your "crown jewels" are, have accurate network diagrams, log access, and internal imaging/collection capabilities.
- ❖ Vet several vendors and negotiate the MSA before an event happens.
 - ❖ Do on-boarding with primary forensic firm before an incident
 - ❖ Review technical incident response capabilities and run books pre-incident.
- ❖ Have a backup – one firm may not be available or appropriate for all events.
- ❖ Retain counsel for incident response that understands technology and cyber issues to reduce response time.
- ❖ Establish protocols to maintain privilege
- ❖ Perform tabletop exercises with your vendors

13

Credit Monitoring

Why Offer?

It mitigates harm, positively changes affected individuals' expectations and regulators' expectations

60%

Offered Credit Monitoring When Notification Occurred

Why Not Offer?

It does not prevent fraudulent charges on payment cards.

- ❖ It may impact litigation position.
- ❖ Low redemption rate.

35%

Average Redemption

BakerHostetler, 2018 Data Security Incident Response Report, (2018)

14

The Importance of Messaging

Goals

- Comply with all applicable laws and regulations
- Be thorough and descriptive without causing unnecessary concern.
- Provide reassurance without overpromising
- Strive for openness and transparency without creating unnecessary risk

Risks

- Complaints
- Negligence, Invasion of Privacy Lawsuits
- Class Action Lawsuits
- Regulatory Action
- Damage to Brand and Trust

15

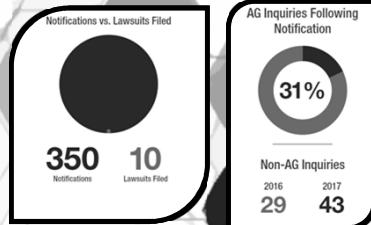
The Importance of Messaging Communication Don'ts

- ❖ Don't speak too early and/or "on the fly."
- ❖ Don't use a misleading initial holding statement
- ❖ Don't fall victim to saying too much or being too reassuring.
- ❖ Don't make logistical mistakes (e.g., call center)
- ❖ Don't assume you have to answer all media inquiries
- ❖ Don't over-apologize
- ❖ Don't leave out helpful evidence
- ❖ Don't call yourself a victim
- ❖ Don't overstate the security measures you had in place.
- ❖ Don't overstate new security measures
- ❖ Don't ignore regulators

16

After You've Mailed Notice...

- ❖ Business may suffer reputational harm.
- ❖ Business may receive AG or OCR inquiries, litigation and regulatory investigations, or a lawsuit.
- ❖ Business operations and a disruption in productivity may result.



17

Rise of the Regulators

- ❖ State Attorney Generals (AGs)
- ❖ Office for Civil Rights (OCR)
- ❖ Other Regulators

31%
AG Inquiries
Following
Notification



Agencies issue Civil Investigative Demands (CIDs) that request:

- ✓ Information Security Plan
- ✓ Remediation Steps
- ✓ Digital Environment Details and its Physical, Technical, and Administrative Controls

18

The Privacy “Patchwork”

- Federal & state laws govern the handling of PII/PHI
 - Laws covering SSNs / disposal of PII
 - Employment-related laws (e.g. FMLA, A
 - Other federal and state regulations (e.g. Mass. Regs)
- HIPAA
 - Applies to Covered Entities and Business Associates
 - Preempted except where state law is “more restrictive”
- State breach notification laws
- State medical information breach regulations
- International data protection regulations



199

HIPAA

Breach by a Covered Entity



- **Applies To:** A health plan, health care clearinghouse and health care provider who transmits any health information in electronic form in connection with a covered transaction.
- **Information Covered:** Unsecured PHI— individually identifiable health information that is transmitted or maintained in electronic media or any other form or media (*encryption=safe harbor*).
- **Definition of Breach:** The acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule, which compromises the security or privacy of the PHI.
- **Who Must Be Notified:** The patient or their personal representative, HHS, and the media if more than 500 residents of a state or jurisdiction are affected.
- **Notification Timeframe:** Without unreasonable delay and in no case later than sixty (60) calendar days after the breach is discovered.
- **Preemption:** HIPAA preempts state law unless state law is more restrictive.

20

Definition of “Breach” in Final Rule

- Acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under the HIPAA Privacy Rule is **presumed** to be a breach. . .
- **Unless** the Covered Entity or Business Associate can demonstrate that there is a **low probability that the PHI has been compromised** based on a risk assessment.
- Compromise is not defined. . .



21

HIPAA Breach Risk Assessment

- Must be documented
- Must evaluate at least the following 4 factors:
 1. The nature and extent of the PHI.
 2. The unauthorized person involved.
 3. Whether the PHI was actually acquired or viewed.
 4. Extent to which any risk has been mitigated.



22

OCR Hot Buttons

- **Recent Focus on Hacking Rel:**
 - Intrusion Detection Software
 - Anti-Virus Software
 - Logging
 - Updating
 - Access Controls
 - Training
- **Mobile Device and Transmis**
 - Encryption
 - Device Inventory, Tracking, and
 - Facility Security and Theft Prev
- **Risk Assessments and Risk M**
- **Third Party Access to PHI / Bu Associates**
- **Staff Education and Sanctions**



OCR Resolution Agreements

- Providence Health & Services (\$100K)
- CVS Pharmacy (\$2.25M)
- Rite-Aid (\$1M)
- Management Services Organization of Washington (\$35K)
- Cignet (\$4.3M)
- Massachusetts General Hospital (\$1M)
- UCLA Health Services (\$865K)
- Blue Cross Blue Shield of Tennessee (\$1.5M)
- Alaska Medicaid (\$1.7M)
- Phoenix Cardiac Surgery, P.C. (\$100K)
- Massachusetts Eye and Ear Infirmary (\$1.5M)
- Hospice of North Idaho (\$50K)
- Idaho State University (\$400K)
- Shasta Regional Medical Center (\$275K)
- WellPoint (\$1.7M)
- Affinity Health Plan (\$1.2M)
- Adult & Pediatric Dermatology, P.C. of Massachusetts (\$150K)
- Skagit County, Washington (\$215K)
- OCA Health Plan, Inc. (\$250K)
- Concentra Health Services (\$1.725M)
- New York and Presbyterian Hospital (\$3.3M)
- Columbia University (\$1.5M)
- Parkview Health System (\$800K)
- Anchorage Community Mental Health Services (\$150K)

24

OCR Resolution Agreements

- Coriell Prescription Pharmacy (\$125K)
- St. Elizabeth's Medical Center (\$216.4K)
- Cancer Care Center (\$750K)
- Lahey Hospital and Medical Center (\$850K)
- Triple-S Management Corporation (\$3.3M)
- University of Washington Medicine (\$750K)
- Lincare (\$239.8K)
- Complete PT, Pool & Land Physical Therapy (\$25K)
- North Memorial Healthcare (\$1.55M)
- Feinstein Institute for Medical Research (\$3.9M)
- Raleigh Orthopaedic Clinic, PA of N. Carolina (\$750K)
- New York Presbyterian Hospital (\$2.2M)
- Catholic Health Care Services of the Archdiocese of Philadelphia (\$650K)
- Oregon Health & Science University (\$2.7M)
- University of Mississippi Medical Center (\$2.75M)
- Advocate Health Care Network (\$5.55M)
- Care New England Health System (\$400K)
- St. Joseph Health (\$2.14M)
- University of Massachusetts Amherst (\$650K)
- Presence Health (\$475K)
- Children's Medical Center of Dallas (\$3.2M)
- Memorial Healthcare System (\$5.5M)
- The Center for Children's Digestive Health (\$31K)
- CardioNet (\$2.5M)
- 21st Century Oncology (\$2.3M)
- Saint Luke's - Roosevelt Hospital Center, Inc. (\$378K)
- Fialta (\$100K)
- University of Texas MD Anderson Cancer Center (\$4.3M)

Exception Medical Care North America (62.8M)

25

State Laws

- 50 States, D.C., & U.S. territories
- Laws vary between jurisdictions
- Varying levels of enforcement by state attorneys general
- Limited precedent



26

International Breach Notification

- ❏ Several Non-U.S. jurisdictions have security breach notification requirements
 - ❏ Some are specific to certain industries.
 - ❏ Some only require notification to a regulator.
- ❏ In certain countries, authorities have issued "guidance" for providing breach notification.
- ❏ GDPR imposes a 72-hour notification requirement.



27

GDPR Breach Notification

"Personal data breach": incident in security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed

Data controller must notify the competent Supervising Authority without undue delay and, where feasible, not later than 72 hours after discovery

If more than 72 hours later, must give reason for delay

Content: (1) Description of incident (number affected, categories of data subjects and data records); (2) DPO contact information; (3) likely consequences of incident, including mitigation efforts

Individual notification required if there's a high risk (with exceptions)

Data processor must notify data controller "without undue delay" but no strict deadline
Entities operating in the EU should prepare a GDPR-compliant data security incident response plan

28

GDPR Applicability

❖ **GDPR only applies to organizations outside of the EU to the extent that they offer goods and services to or monitor the behavior of EU data subjects.**

❖ **Key Questions**

❖ **1. Offering goods in services**

❖ Do you have any representatives or offices in the EU?

❖ Does your website have a domain with an EU extension (e.g. .fr, .es, .de)?

❖ Do you provide a telephone number with an EU country code?

❖ Do any of your promotional or marketing materials mention EU-based clientele?

❖ **2. Monitoring the behavior of EU data subjects**

❖ Do you track subjects on the internet (e.g. cookies)?

❖ Do you use data processing techniques to profile data subjects, their behaviors or attitudes?

29

Is California the Next GDPR?

California Consumer Privacy Act of
June 28, 2018

• Takes effect June 2020

• Stated Purpose:

• to give consumers more control and transparency regarding use of private information.

• Recent amendments would prohibit application of act to PHI collected by HIPAA-covered entities; however, may still apply to other types of personal information.

30


RISK MANAGEMENT STRATEGIES

PREVENTION = PROTECTION

- Vendor Management
- Security Awareness/Education
- Basic Data Security Good Practices
- Risk Assessment, Risk Management Plan
- Policies and Procedures
- Consistent Enforcement of Policies and Procedures
- Practice breach response initiative
- Delete data when it is no longer needed

BASIC DATA SECURITY BEST PRACTICES

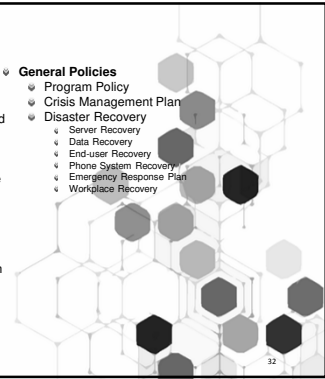
- Data Identification & Classification
- Data hygiene don't collect what you don't need)
- Access restrictions
- Education
- Document retention/destruction



31

Policy & Procedures

- Security Incident Response Plan
- BYOD Policy and Social Media Policy
- Information Security and User Policies
 - What users can and must do to use network and organization's computer equipment.
 - Define limitations on users to keep the network secure (password policies, use of proprietary information, internet usage, system use, remote access)
- IT Policies
 - Virus incident and security incident
 - Logs
 - Backup policies
 - Server configuration, patch update, modification policies
 - Firewall policies
 - Wireless, VPN, router, and switch security
 - Email retention
- General Policies
 - Program Policy
 - Crisis Management Plan
 - Disaster Recovery
 - Server Recovery
 - Data Recovery
 - End-user Recovery
 - Phone System Recovery
 - Emergency Response Plan
 - Workplace Recovery



32

Questions



33
